KONICA MINOLTA

The essentials of imaging

bizhub 362/282/222

User's Guide [Security Operations]

2009. 6
Ver. 1.01

Contents

1 Security

1.1 Introduction 1-2
Compliance with the ISO15408 Standard 1-2
Operating Precautions 1-2
INSTALLATION CHECKLIST 1-4

1.2 Security Functions 1-6

1.2.1 Check Count Clear Conditions 1-7

1.3 Data to be Protected 1-8

1.4 Precautions for Operation Control 1-9
Roles and Requirements of the Administrator 1-9
Password Usage Requirements 1-9
Network Connection Requirements for the Machine 1-10
Security function operation setting operating requirements 1-10
Operation and control of the machine 1-10
Machine Maintenance Control 1-10

1.5 Miscellaneous 1-11
Password Rules 1-11
Precautions for Use of Various Types of Applications 1-11

2 Administrator Operations

2.1 Accessing the Admin. Management Mode 2-2

2.1.1 Accessing the Admin. Management mode 2-2
<From the Control Panel> 2-3
<From PageScope Web Connection> 2-5

2.2 Enhancing the Security Function 2-8

2.2.1 Setting the Enhance Security function 2-10
<Setting can be made only from the control panel> 2-10

2.3 Canceling the Access Lock State 2-13

2.3.1 Performing Unlock Setting 2-14
<Setting can be made only from the control panel> 2-14

2.4 Changing the Administrator Code (Administrator Password) 2-15

2.4.1 Changing the Administrator Code (Administrator Password) 2-15
<Setting can be made only from the control panel> 2-15

2.5 User Box Function 2-19

2.5.1 Changing the User Box Number and User Box Password 2-19
<Setting can be made only from the PageScope Web Connection> 2-19

2.6 Protecting Data in the HDD 2-24

2.6.1 Setting the HDD Lock Password 2-25
<Setting can be made only from the control panel> 2-25

2.6.2 Changing the HDD Lock Password 2-30
<Setting can be made only from the control panel> 2-30

2.6.3 Setting the Encryption Key (encryption word) 2-34
<Setting can be made only from the control panel> 2-34

2.6.4 Changing the Encryption key 2-39
<Setting can be made only from the control panel> 2-39

2.7 Overwrite All Data Function 2-45

2.7.1 Executing Overwrite All Data 2-46
<Setting can be made only from the control panel> 2-46

2.8 Network Setting Function 2-47

2.8.1 Setting the IP Address 2-47
<From the Control Panel> 2-47
<From PageScope Web Connection> 2-48

2.8.2 Making the NetWare setting 2-48
<From PageScope Web Connection> 2-48

2.8.3 Making the Windows print (NetBIOS) setting 2-49
<From PageScope Web Connection> 2-49

2.8.4 Making the AppleTalk setting 2-49
<From PageScope Web Connection> 2-49

3 User Operations

3.1 Secure Print Function 3-2

3.1.1 Accessing the Secure Print 3-2
<Setting can be made only from the control panel> 3-3

3.2 User Box Function 3-6

3.2.1 Setting the User Box 3-6
<Setting can be made only from PageScope Web Connection> 3-6

3.2.2 Accessing a User Box document 3-10
<From the Control Panel> 3-10
<From PageScope Web Connection> 3-13

3.2.3 Changing the User Box Number and User Box Password 3-18
<Setting can be made only from PageScope Web Connection> 3-18

1 Security

1 Security

1.1 Introduction

Thank you for purchasing our product.

This User's Guide contains the operating procedures and precautions to be used when using the security functions offered by the bizhub 362, 282, or 222 machine. To ensure the best possible performance and effective use of the machine, read this manual thoroughly before using the security functions. The Administrator of the machine should keep this manual for ready reference. The manual should be of great help in finding solutions to operating problems and questions.

This User's Guide (Ver. 1.01) describes bizhub 350/bizhub 250/bizhub 200/ bizhub 362/bizhub 282/bizhub 222/ineo 362/ineo 282/ineo 222/VarioLink 3621/VarioLink 2821/VarioLink 2221 Multi Function Peripheral Control Software (MSC: A11U-0100-G10-06).

Compliance with the ISO15408 Standard

When the Enhance Security function on this machine is set to [ON], more enhanced security functions are available.

The security functions offered by the bizhub 362, 282, or 222 machine comply with ISO/IEC15408 (level: EAL3).

Operating Precautions

This machine issues an alarm message or sounds an alarm beep when it is erroneously operated or wrong data is entered. (The alarm beep is not, however, sounded if Confirmation Beep of User Management is set to [0].) If the alarm message appears or the alarm beep sounds, follow the instructions given by the message and operate the machine correctly or input correct data as necessary.

The Administrator of the machine should make sure that each individual general user exits from the current mode to return to the basic screen whenever the access to that mode is completed or if the user leaves the machine with the mode screen left displayed.

The Administrator of the machine should exit from the current mode to return to the basic screen whenever the access to that mode is completed or if he or she leaves the machine with the mode screen left displayed.

The Administrator of the machine should make sure that none of the One-Touch Names to be used for a one-touch key is not duplicated when making settings for the one-touch key used for Scan to HDD on the machine. If a One-Touch Name is duplicated, data could be saved in a wrong User Box. If there are two or more User Boxes having the same User Box Name, the Administrator should make doubly certain that the correct User Box is registered for a one-touch key.

INSTALLATION CHECKLIST

This Installation Checklist contains items that are to be check by the Service Engineer installing this machine.
The Service Engineer should check the following items, then explain each checked item to the Administrator of the machine.

To Service Engineer

Make sure that each of these items is properly carried out by checking the box on the right of each item.

		Completed
1.	Perform the following steps before installing this machine.	
	Check with the Administrator to determine if the security functions of this machine should be enhanced. If the functions should be enhanced, check the following. If the security functions are not to be enhanced, quit the operation without checking the following.	☐
	I swear that I would never disclose information as it relates to the settings of this machine to anybody, or perform malicious or intentional act during setup and service procedures for the machine.	☐
	When giving the User's Guide Security Operations to the Administrator of the machine, check that the User's Guide is the security-compatible version and explain to the Administrator that it is security-compatible.	☐
2.	After this machine is installed, refer to the Service Manual and perform the following steps.	
	Check that the Firmware version (MSC) indicated in the Service Manual matches the values shown in the Firmware Version screen. If there is a mismatch in the Firmware version number, explain to the Administrator of the machine that upgrading of the Firmware is necessary and perform upgrading of the Firmware.	☐
	Set the Service Code.	☐
	Check that CS Remote Care is set to disabled (RAM Clear).	☐
3.	After this machine is installed, refer to this User's Guide and perform the following steps.	
	Check that the Administrator Code (Administrator Password) has been set by the Administrator of the machine.	☐
	Check that the self-signed certificate for SSL communications has been registered by the Administrator of the machine. (PageScope Web Connection cannot be used if the self-signed certificate is yet to be registered.)	☐
	If the optional Hard Disk HD-504 and Security Kit SC-504 are mounted, check that the HDD Lock Password or Encryption Key, or both, have been registered by the Administrator of the machine.	☐
	Let the Administrator of the machine set Enhance Security function to [ON].	☐
	The language, in which the contents of the User's Guide Security Operations have been evaluated, is English. Explain the way how to get the manual in the language, in which it is evaluated.	☐
	Explain to the administrator that the settings for the security functions for this machine have been specified.	☐

When the above steps have been properly carried out, the Service Engineer should make a copy of this page and give the original of this page to the Administrator of the machine. The copy should be kept at the corresponding Service Representative for filing.

Product Name		Company Name	User Division Name	Person in charge
Customer				
Service Representative			-	

1.2 Security Functions

Setting the Enhance Security function to [ON] will validate the security function of this machine. For details of the settings of different security functions to be changed by turning [ON] the Enhance Security function, see “Enhancing the Security Function” on page 2-8.

Setting the Enhance Security function to [ON] will enhance the authentication function. Access control is then provided through password authentication for any access to the Admin. Management mode, User Box, a User Box data file, and a Secure Print file. Access is thereby granted only to the authenticated user.

A password that can be set must meet the requirements of the Password Rules. The machine does not accept setting of an easily decipherable password. For details of the Password Rules, see “Password Rules” on page 1-11.

If a wrong password is entered three times during the password authentication procedure, the machine determines that it is unauthorized access through the failed access penalty function, prohibiting any further entry of the password. By prohibiting the password entry operation, the machine prevents unauthorized use or removal of data, thereby ensuring secured used of the machine.

To cancel the password entry operation prohibited condition, the Administrator must perform the Unlock. When the Administrator performs the Unlock for the operation prohibited condition, a sound operation control in utmost security is achieved under the control of the Administrator.

If the optional Hard Disk HD-504 is mounted, the HDD Lock Password setting provides the following security function. That is, even if the HDD is illegally and secretly replaced with another, the HDD authentication function prohibits access to the HDD, when the HDD Lock Password is yet to be set or there is a mismatch in the passwords. In addition, should the HDD be removed unawares, the HDD Lock Password locks the HDD protecting data contained in the HDD. Furthermore, by mounting the optional Security Kit SC-504 and setting the Encryption Key, the data stored in the HDD is encrypted, thereby protecting the data in the HDD. Note, however, that the HDD Lock Password and Encryption Key do not prevent the HDD from being physically removed. Make sure of a good operation control.

When the machine is to be discarded, or use of a leased machine is terminated at the end of the leasing contract, the Overwrite All Data function overwrites and erases all data stored in all spaces of the HDD. The function also resets all passwords saved in the NVRAM to factory settings, preventing leak of data. For details of items to be cleared by Overwrite All Data function, see “Overwrite All Data Function” on page 2-45.

1.2.1 Check Count Clear Conditions

The following are the conditions for clearing or resetting the check count of the number of wrong entries at the time of authentication by the Enhance Security function.

<Admin. Management mode>
- Authentication of Admin. Management mode is successful.
- Authentication for executing the Administrator Code (Administrator Password) Input function is successful.
- The machine is restarted.

<Secure Print>
- Authentication of Secure Print is successful.
- Unlock function is executed.

<User Box>
- Unlock function is executed.
- Authentication for execution of change of User Box Number, User Box Name, and User Box Password is successful.
- Authentication of User Box is successful.
- Authentication for acquiring scan data files is successful.
- The machine is restarted.

1.3 Data to be Protected

The underlying concept of this machine toward security is “to protect data that can be disclosed against the intention of users.”

The following types of image files that have been stored in the machine and made available for use by its users are protected while the machine is being used.

- Image files stored by Secure Print
- Image files stored in User Box (except for Public User Box)

The following types of data stored in the HDD are protected when use of a leased machine is terminated at the end of the leasing contract, the machine is to be discarded, or when the HDD is stolen.

- User Box files
  (including those saved in the Public User Box)
- Swap data files
  – Generated in a copy, PC print, or Secure Print Document that is too large in size to fit in the RAM space
- Overlay image files
  – Background image files
  – A copy can be made with this image file to be registered set in the background
- HDD stored image files
  – Files stored in the HDD from copy and PC print and printed through operations from the control panel
- Remaining image files
  – Files that are not erased through ordinary file deleting operations and are left in the data space
- Destination recipient data files
  – Files including e-mail addresses and telephone numbers

1.4 Precautions for Operation Control

This machine and the data handled by this machine should be used in an office environment that meets the following conditions.

Roles and Requirements of the Administrator

The Administrator should take full responsibility for controlling the machine, thereby ensuring that no improper operations are performed.

<To Achieve Effective Security>

- A person who is capable of taking full responsibility for controlling the machine should be appointed as the Administrator to make sure that no improper operations are performed.

Password Usage Requirements

The Administrator must control the Administrator Code (Administrator Password), HDD Lock Password, and Encryption Key appropriately so that they may not be leaked. These passwords should not be ones that can be easily guessed. The user, on the other hand, should control the User Box Password and Secure Print Password appropriately so that they may not be leaked. Again, these passwords should not be ones that can be easily guessed. For the User Box shared among a number of users, the User Box Password should be appropriately controlled so that it may not be leaked to anyone who is not the user of the User Box.

<To Achieve Effective Security>

- Make absolutely sure that only the Administrator knows the Administrator Code (Administrator Password), HDD Lock Password, and Encryption Key.
- The Administrator must change the Administrator Code (Administrator Password), HDD Lock Password, and Encryption Key at regular intervals.
- The Administrator should make sure that any number that can easily be guessed from birthdays, employee identification numbers, and the like is not set for the Administrator Code (Administrator Password), HDD Lock Password, and Encryption Key.
- If a User Box Password has been changed, the Administrator should have the corresponding user change the User Box Password as soon as possible.
- If the Administrator Code (Administrator Password) has been changed by the Service Engineer, the Administrator should change the Administrator Code (Administrator Password) as soon as possible.
- The Administrator should have users ensure that the Secure Print Password is known only by the user concerned.
- The Administrator should make sure that only the users who share a User Box know the User Box Password set for it.
- The Administrator should have users change the User Box Passwords set for User Boxes at regular intervals.

- The Administrator should make sure that any user does not set any number that can easily be guessed from birthdays, employee identification numbers, and the like for passwords set for Secure Print and User Box.

Network Connection Requirements for the Machine

Packets being transmitted over the LAN installed in the office, in which the machine is installed, should be protected from unauthorized manipulation. If the LAN is to be connected to an outside network, no unauthorized attempt to establish connection from the external network should be permitted.

<To Achieve Effective Security>

- If the LAN, in which the machine is installed, is connected to an outside network, install a firewall or similar network device to block any access to the machine from the outside network and make the necessary settings.
- Configure the LAN installed in the office, in which the machine is installed, by using a switching hub and other devices to ensure that the packets are protected from unauthorized manipulation.

Security function operation setting operating requirements

The Administrator should make sure of correct operation control so that the machine is used with the Enhance Security function set to [ON].

Operation and control of the machine

The Administrator of the machine should perform the following operation control.

- The Administrator of the machine should log off from the Admin. Management mode whenever the operation in the Admin. Management mode is completed.
- The Administrator should have users make it a rule to return to the Basic screen whenever the operation for the Secure Print file and User Box file have been completed.

Machine Maintenance Control

The Administrator of the machine should perform the following maintenance control activities.

- Provide adequate control over the machine to ensure that only the Service Engineer is able to perform physical service operations on the machine.
- Provide adequate control over the machine to ensure that any physical service operations performed on the machine by the Service Engineer are overseen by the Administrator of the machine.

1.5 Miscellaneous

Password Rules

According to certain Password Rules, registration of a password consisting of a string of a single character or change of a password to one consisting of a string of a single character is rejected for the Administrator Code (Administrator Password), User Box Password, Secure Print Password, HDD Lock Password, and Encryption Key.

Study the following table for more details of the number of digits and characters that can be used for each password.

Types of passwords	No. of digits	Characters
Administrator Code (Administrator Password)	8 digits	• Numeric characters: 0 to 9 Selectable from among a total of 10 characters
User Box Password		• Numeric characters: 0 to 9 • Alpha characters: upper and lower case letters • Symbols: !, #, $, %, &, ', (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [, \,], _, `, {, |, }, ~, SPACE Selectable from among a total of 92 characters
Secure Print Password		
HDD Lock Password	20 digits	• Numeric characters: 0 to 9 • Alpha characters: upper and lower case letters • Symbols: !, #, $, %, &, ', *, +, -, ., /, =, ?, @, _, `, {, |, }, ~ Selectable from among a total of 82 characters
Encryption Key		

Precautions for Use of Various Types of Applications

When PageScope Web Connection or an application of various other types is used, the password control function of the application stores the password that has been entered in your PC. If you want the password not stored, disable the password control function of the application.

The Administrator of the machine should explain to users the following precautions and make sure that they follow these precautions. That is, when using the PageScope Web Connection or an application of various other types, the user should use one that shows "*" or "●" for the password entered.

2 Administrator Operations

2 Administrator Operations

2.1 Accessing the Admin. Management Mode

This machine implements authentication of the user of the Admin. Management mode function through the 8-digit Administrator Code (Administrator Password) that verifies the identity as the Administrator of the person who accesses the function. During the authentication procedure, the Administrator Code (Administrator Password) entered for the authentication purpose appears as "*" or "●" on the display.

When the Enhance Security function is set to [ON], the number of times in which authentication fails is counted.

2.1.1 Accessing the Admin. Management mode

...

Note

Never forget the Administrator Code (Administrator Password). If the Administrator Code (Administrator Password) is forgotten with the Enhance Security function set to [ON], it becomes impossible to set the Administrator Code (Administrator Password) again. Contact your Service Representative.

Make sure that none of the general users of the machine will know the Administrator Code (Administrator Password).

If the Administrator Code (Administrator Password) is forgotten, it must be set again by the Service Engineer. Contact your Service Representative.

Do not leave the machine with the Admin. Management mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin. Management mode.

...

Reminder

If another Administrator has already logged on to the Admin. Management mode using PageScope Web Connection and you attempt to access the Admin. Management mode from the control panel, a message appears that tells something to the effect that all operations are currently disabled due to registration being made over the network. Wait until the message disappears before attempting once again to access the Admin. Management mode.

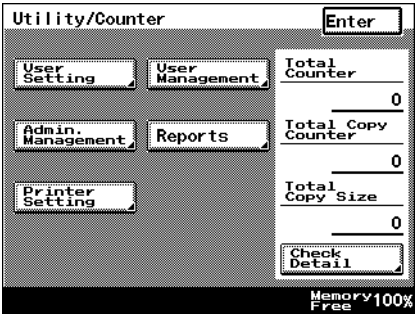
<From the Control Panel>

1 Press the [Utility/Counter] key.

2 Touch [Admin. Management].

? Is it possible to gain access to the Admin. Management mode while a job is being executed?

➔ The machine does not accept access to the Admin. Management mode while a job is being executed. Wait until the execution of the job is completed before attempting to access the Admin. Management mode again.



3 Enter the 8-digit Administrator Code (Administrator Password) from the keypad.

– Press the [C] key to clear all characters.
– Touch [Cancel] to go back to the screen shown in step 2.

4 Touch [Enter].

? What happens if a wrong Administrator Code (Administrator Password) is entered?

➔ If a wrong Administrator Code (Administrator Password) is entered, a message appears saying that the password entered is wrong. Enter the correct Administrator Code (Administrator Password).

➔ If the Enhance Security function is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Code (Administrator Password) is entered three times, a message appears that tells that the machine accepts no more Administrator Codes (Administrator Passwords) because of unauthorized access for any subsequent entry of the Administrator Code (Administrator Password). The machine is then set into an access lock state. To cancel the access lock state, turn off, and then turn on, the main power switch of the machine. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. Be sure to allow an interval of 10 sec. or more in order to ensure correct operations.
Here is the sequence, through which the main power switch and sub power switch are turned on and off:
Turn off the sub power switch → Turn off the main power switch → Turn on the main power switch → Turn on the sub power switch

5 Press the [Reset] key to log off from the Admin. Management mode.

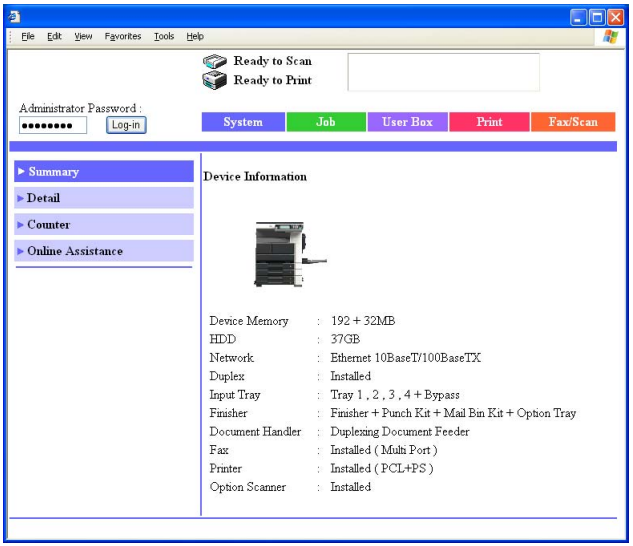
<From PageScope Web Connection>

1 Start the Web browser.

2 Enter the IP address of the machine in the address bar.

3 Press the [Enter] key to start PageScope Web Connection.

4 Enter the 8-digit Administrator Code (Administrator Password) in the "Administrator Password" box.



? What is the Administrator Code (Administrator Password) used for accessing the Admin. Management mode via the PageScope Web Connection?

➔ When accessing the Admin. Management mode using the PageScope Web Connection, enter the same Administrator Code (Administrator Password) as that for the machine.

5 Click the [Log-in].

? What happens if a wrong Administrator Code (Administrator Password) is entered?

➔ If a wrong Administrator Code (Administrator Password) is entered, a message appears saying that the password entered is wrong. In this case, click [OK] and enter the correct Administrator Code (Administrator Password) in the "Administrator Password" box.

➔ If the Enhance Security function is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Code (Administrator Password) is entered three times, a message appears that tells that the machine accepts no more Administrator Codes (Administrator Passwords) because of unauthorized access for any subsequent entry of the Administrator Code (Administrator Password). The machine is then set into an access lock state. To cancel the access lock state, turn off, and then turn on, the main power switch of the machine. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. Be sure to allow an interval of 10 sec. or more in order to ensure correct operations.
Here is the sequence, through which the main power switch and sub power switch are turned on and off:
Turn off the sub power switch → Turn off the main power switch → Turn on the main power switch → Turn on the sub power switch

? Is it possible to gain access to the Admin. Management mode while a job is being executed?

➔ If an attempt is made to log on to the Admin. Management mode while a job is being executed, the machine gives a message that tells that it is now impossible to log on to the Admin. Management mode. Click [OK] and try logging on to the Admin. Management mode after the execution of the job is completed.

? What happens if another Administrator has logged on to the Admin. Management mode using PageScope Web Connection?

➔ If you have already logged on to the Admin. Management mode using PageScope Web Connection, no operations can be made on the control panel of the machine. If another Administrator has logged on to the Admin. Management mode using PageScope Web Connection, a message appears that tells that there is some other Administrator who has already logged on to the Admin. Management mode. Then, the machine does not accept any attempt to log on to the Admin. Management mode from PageScope Web Connection.

➔ If no operations are performed for 10 min. while the machine is in the Admin. Management mode, you will automatically log off from the Admin. Management mode.

6 Click the [Logout].

This allows you to log off from the Admin. Management mode.

Note

If you have logged on to the Admin. Management mode using the PageScope Web Connection and if you close the web browser without clicking [Logout], the touch panel of the machine remains locked for 70 sec.

2.2 Enhancing the Security Function

When access to the Admin. Management mode by the Administrator of the machine via the control panel is authenticated, the machine enables setting of the Enhance Security function that allows settings for enhancing each of different security functions to be converted all at once.

In the Enhance Security function, the machine allows selection of whether to use the Enhance Security function or not. If the Enhance Security function is set to [ON], a count is taken of the number of unauthorized accesses to the Admin. Management mode, all Secure Prints, and all User Boxes. A function is also set that determines whether each password meets predetermined requirements. The security function is thus enhanced in the Enhance Security function.

The following settings must first be made before the Enhance Security function is set to [ON].

Note

Assume a condition, in which the machine has been used with the optional Hard Disk HD-504 mounted and the Encryption Key is to be newly set as a result of mounting of the Security Kit SC-504 on the machine. In such a condition, it becomes necessary for you to set the HDD Lock Password also. Setting the Encryption Key erases data in the HDD because of HDD formatting. It is recommended that the data be backed up in advance.

When the Enhance Security function is to be turned [ON], the Administrator of the machine should make sure that all users, for whom User Boxes are controlled, have changed the User Box Passwords to those that meet the requirements of the Password Rules in advance. For details of Password Rules, see "Password Rules" on page 1-11.

Settings to be Made in Advance	Description
Administrator Code (Administrator Password)	An 8-digit password that meets the Password Rules. The factory setting is "12345678."
HDD Lock Password, Encryption Key	If the optional Hard Disk HD-504 and Security Kit SC-504 are mounted, be sure to set the 20-digit HDD Lock Password or Encryption Key, or both.
Certificate for SSL	Register the self-signed certificate for SSL communications.
Service Code	Calls for setting made by the Service Engineer. For details, ask your Service Representative.
CS Remote Care	

Setting the Enhance Security function to [ON] changes the setting values of the following functions.

Function Name	Factory Setting	When Enhance Security function is set to [ON]
Software SW	Available on screen	Not available on screen (not to be changed) The setting values of the following functions of Software SW are changed as detailed below: • Password Rules: For details of Password Rules, see "Password Rules" on page 1-11. Set to ON. • Access Lock: Detects the number of failed authentication attempts for the Admin. Management mode, Secure Print, and User Box. Set to ON (setting the machine in an access lock state at three failed authentication attempts). (When Access Lock is set to ON, it sets an additional function of requiring authentication for a downloading operation of a box document.) • Temporary Data Overwriting: Delete by overwriting data and temporary files that are saved in the HDD and memory, but that are no longer necessary. Overwrites with 0x00 → 0x00 → 0x00. Set to ON. • Secure Print Access Method: The method of accessing Secure Print can be selected. A method is set, in which authentication is made by means of the Secure Print Password after the relevant Secure Print documents have been narrowed down using Secure Print ID. • TCP socket: Setting can be made as to whether transmission of data using the TCP socket is allowed or not. Prohibited is set. When Software SW is not available on the screen, however, the setting values of the above functions cannot be changed.
Password Rules	OFF	
Access Lock	OFF	
Temporary Data Overwriting	OFF	
Secure Print Access Method	Displays all Secure Print documents that are identified and authenticated by a specified Secure Print ID and Secure Print password	
Prohibit TCP socket	Allow	
SNMP Setting	Enable	Enable * Use of "Private" (Read/Write) of Community Name becomes disabled.
Delete Password (HDD Lock Password)	Available on screen	Not available on screen (not to be changed) * Either the HDD Lock Password or Encryption Key can be deleted if both have been set with the optional Security Kit SC-504 mounted on the machine.

The Temporary Data Overwriting function is executed at the following timing.

- Upon completion of a job, including copy, print, fax, scan and send (scan to E-mail, scan to FTP, scan to SMB)
- A box file or image data stored in the HDD is deleted
- Data is automatically deleted through the setting of User Box Documentation Delete Time
- The main power switch is turned OFF, and then turned ON again during the execution of a job

...

Reminder

When Password Rules is set to [ON], the characters and the number of digits used for each password are restricted. For details of Password Rules, see "Password Rules" on page 1-11.

2.2.1 Setting the Enhance Security function

...

Note

When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. Be sure to allow an interval of 10 sec. or more in order to ensure correct operations.
Here is the sequence, through which the main power switch and sub power switch are turned on and off:
Turn off the sub power switch → Turn off the main power switch → Turn on the main power switch → Turn on the sub power switch

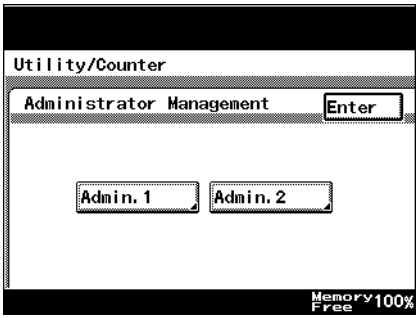
Do not leave the machine with the Admin. Management mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin. Management mode.

<Setting can be made only from the control panel>

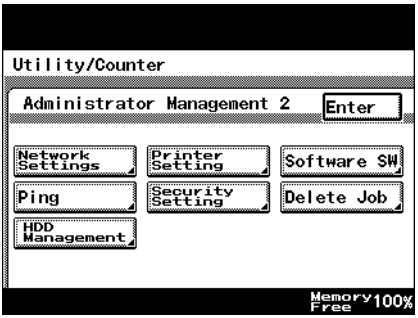
✔ For the procedure to call the Admin. Management mode to the display, see "Accessing the Admin. Management mode" on page 2-2.

1 Call the Admin. Management mode to the screen from the control panel.

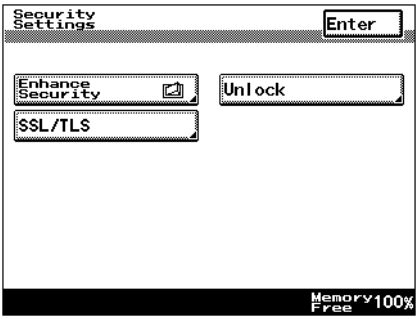
2 Touch [Admin. 2].



3 Touch [Security Setting].



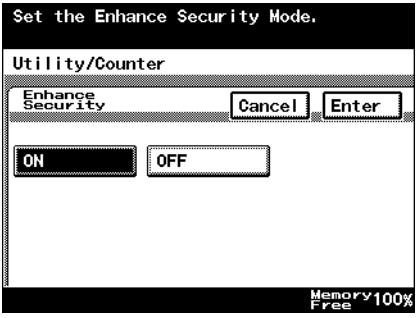
4 Touch [Enhance Security].



5 Touch [ON] to enable the Enhance Security function.

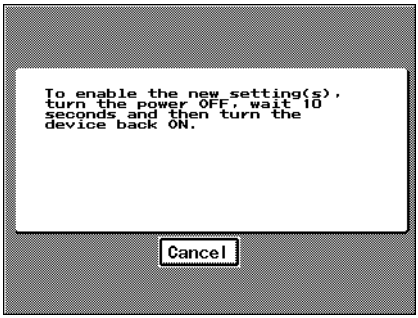
? What is the factory setting for the Enhance Security function?

➔ The Enhance Security function is factory-set to [OFF]. Be sure to turn [ON] the Enhance Security function so as to enable the security function of the machine.



6 Touch [Enter].

7 Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch.



...

Reminder

When the Enhance Security function is set properly, a key icon appears at a lower corner of the screen, indicating that the enhanced security is active.

2.3 Canceling the Access Lock State

When access to the Admin. Management mode by the Administrator of the machine via the control panel is authenticated, the machine enables the operation of the Unlock function so that an access lock state as a result of unauthorized access can be canceled.

The Unlock function clears the unauthorized access check count for all Secure Print authentication and User Box authentication, resetting it to zero.

Perform the following procedure to cancel the password entry prohibited state.

- Admin. Management mode: Turning OFF/ON the main power switch
- Secure Print authentication: Unlock
- User Box authentication: Unlock or turning OFF/ON the main power switch

...

Note

Turning OFF and then turning ON the main power switch deletes the Secure Print Document data and accumulated documents. Make doubly certain of the outcome before turning OFF and ON the main power switch.

When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. Be sure to allow an interval of 10 sec. or more in order to ensure correct operations.
Here is the sequence, through which the main power switch and sub power switch are turned on and off:
Turn off the sub power switch → Turn off the main power switch → Turn on the main power switch → Turn on the sub power switch

2.3.1 Performing Unlock Setting

...

Note

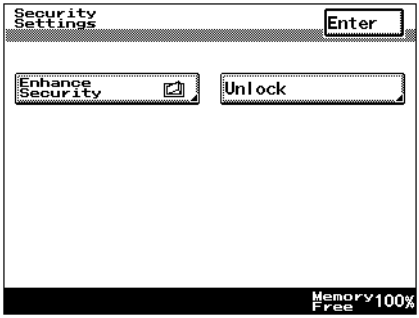
Do not leave the machine with the Admin. Management mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin. Management mode.

<Setting can be made only from the control panel>

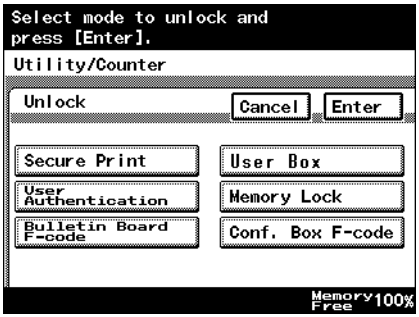
✔ For the procedure to call the Security Settings to the display, see steps 1 through 3 of "Setting the Enhance Security function" on page 2-10.

1 Call the Security Settings to the screen from the control panel.

2 Touch [Unlock].



3 Select the function, for which Prohibit Function as a result of unauthorized access is to be unlocked.



4 Touch [Enter].

This clears the unauthorized access check count of the specific function selected in step 3.

2.4 Changing the Administrator Code (Administrator Password)

When access to the Admin. Management mode from the control panel by the Administrator of the machine is authenticated, the machine enables the operation of changing the Administrator Code (Administrator Password) required for accessing the Admin. Management mode.

The Administrator Code (Administrator Password) entered for the authentication purpose appears as "*" on the display.

Note

Be sure to enter an Administrator Code (Administrator Password) that meets the Password Rules for Administrator Code (Administrator Password). For details of Password Rules, see "Password Rules" on page 1-11.

If the Enhance Security function is set to [ON] after an Administrator Code (Administrator Password) that does not meet the requirements of the Password Rules, the machine regards any subsequent access for Administrator authentication as unauthorized access. As a result, access to the Admin. Management mode can no longer be made. Contact your Service Representative.

2.4.1 Changing the Administrator Code (Administrator Password)

Note

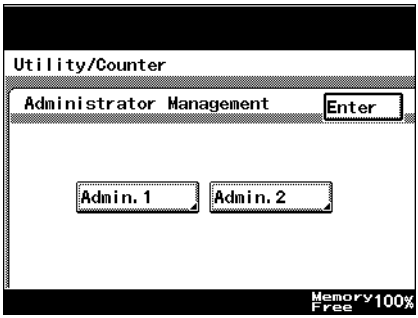
Do not leave the machine with the Admin. Management mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin. Management mode.

<Setting can be made only from the control panel>

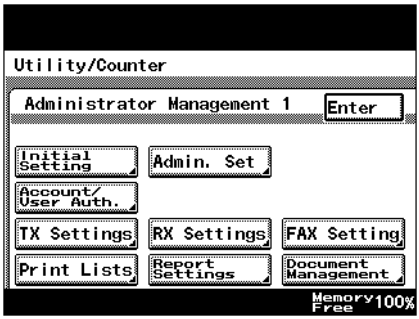
✔ For the procedure to call the Admin. Management mode to the display, see steps 1 through 4 of "Accessing the Admin. Management mode" on page 2-2.

1 Call the Admin. Management mode to the screen from the control panel.

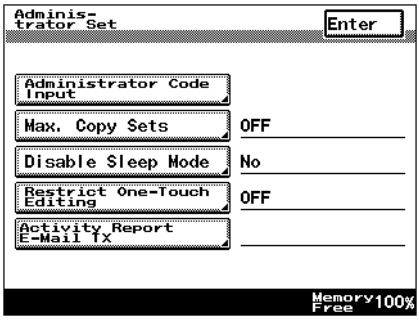
2 Touch [Admin. 1].



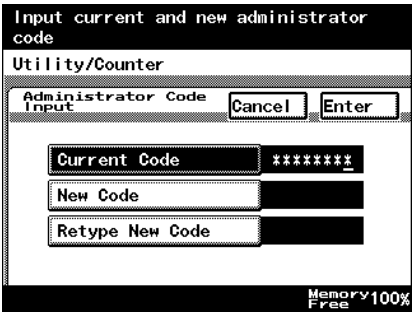
3 Touch [Admin. Set].



4 Touch [Administrator Code Input].

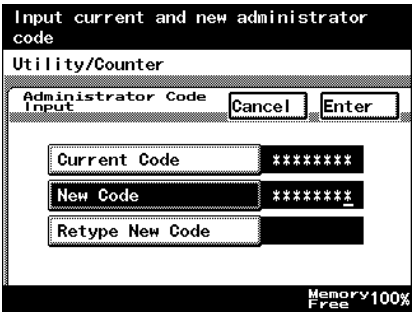


5 Touch [Current Code] and type the currently set 8-digit Administrator Code (Administrator Password) from the keypad.



- Press the [C] key to clear all characters.
- Touch [Cancel] to go back to the screen shown in step 4.

6 Touch [New Code] and type the new 8-digit Administrator Code (Administrator Password) from the keypad.

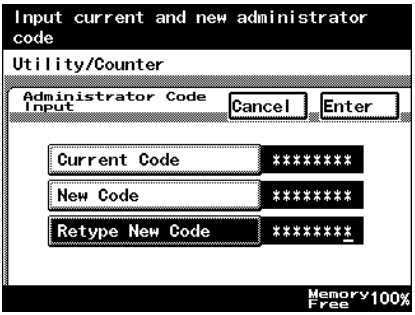


- Press the [C] key to clear all characters.
- Touch [Cancel] to go back to the screen shown in step 4.

? What precautions should be used when entering the new Administrator Code (Administrator Password)?

➔ Be sure to enter an Administrator Code (Administrator Password) that meets the requirements of the Password Rules for the new Administrator Code (Administrator Password). For details of Password Rules, see “Password Rules” on page 1-11.

7 Touch [Retype New Code] and type the new 8-digit Administrator Code (Administrator Password) a second time to prevent entry of a wrong code.



- Press the [C] key to clear all characters.
- Touch [Cancel] to go back to the screen shown in step 4.

8 Touch [Enter].

? What if an Administrator Code (Administrator Password) different from that which is currently registered is mistakenly entered?

➔ If there is a mismatch between the currently registered Administrator Code (Administrator Password) and that which is entered, the machine counts it as unauthorized access.

➔ If there is a mismatch between the currently registered Administrator Code (Administrator Password) and that which is entered, the Utility/Counter screen appears. Perform steps 1 through 8.

? What happens if the Administrator Code (Administrator Password) entered does not meet the requirements of Password Rules?

➔ If the Administrator Code (Administrator Password) entered in [New Code] does not meet the requirements of Password Rules, a message appears that tells that a mismatch is noted in the Administrator Code (Administrator Password) entered. Perform steps 5 through 8 again. For details of Password Rules, see “Password Rules” on page 1-11.

? What happens if there is a mismatch in the Administrator Codes (Administrator Passwords)?

➔ If there is a mismatch between the Administrator Code (Administrator Password) entered in [New Code] and that which is entered in [Retype New Code], a message appears that tells that there is a mismatch in the Administrator Codes (Administrator Passwords). Perform steps 5 through 8 again.

...

Note

Never forget the Administrator Code (Administrator Password). If the Administrator Code (Administrator Password) is forgotten with the Enhance Security function set to [ON], it becomes impossible to set the Administrator Code (Administrator Password) again. Contact your Service Representative.

2.5 User Box Function

When access to the Admin. Management mode using PageScope Web Connection by the Administrator of the machine is authenticated, the machine allows the User Box Number, User Box Password, and User Box Name to be changed.

A User Box Password may consist of 8 digits. The User Box Password entered is displayed as "*" or "●."

Note

The Administrator of the machine should control the User Box Number, User Box Name, and User Box Password for the User Box created by the user.

2.5.1 Changing the User Box Number and User Box Password

Note

Do not leave the machine with the Admin. Management mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log-out from the Admin. Management mode.

When a User Box Name is to be changed, do not use "Public" for the User Box Name to avoid confusion with the "Public User Box" previously registered.

It is not allowed to duplicate any User Box Number that has previously been registered.

NEVER forget the new User Box Number.

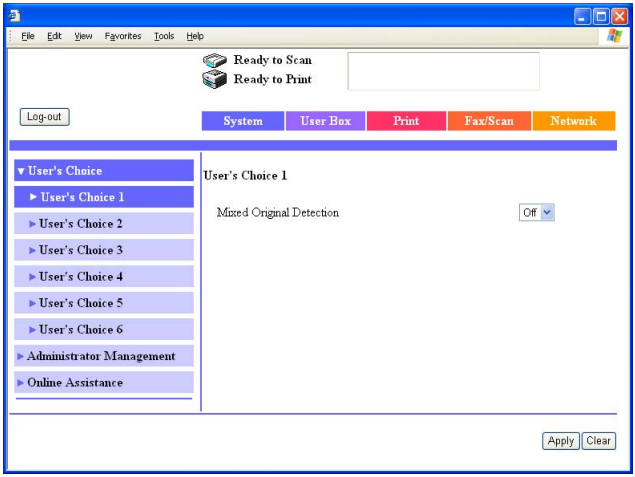
If a User Box Number and a User Box Password have been changed, all users who use the corresponding User Box must be informed of the new User Box Number and the new User Box Password as soon as possible.

<Setting can be made only from the PageScope Web Connection>

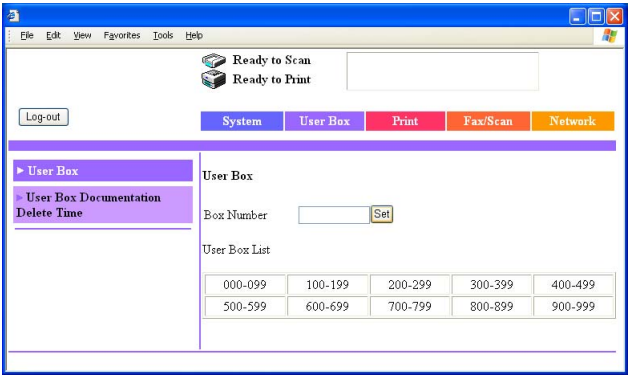
✔ For the procedure to access the Admin. Management mode, see "Accessing the Admin. Management mode" on page 2-2.

1 Start PageScope Web Connection and access the Admin. Management mode.

2 Click the [User Box] tab.



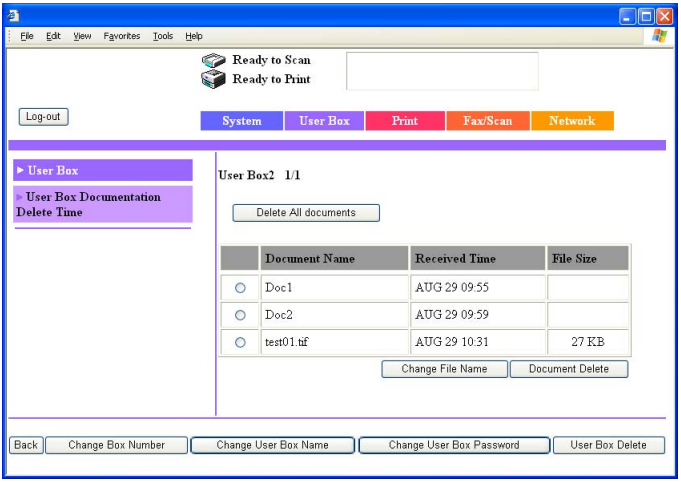
3 Click [User Box] and type the desired User Box Number in the “Box Number” field.



– Clicking a number range index under User Box List will display a list of boxes having the box numbers that fall within the number range index.

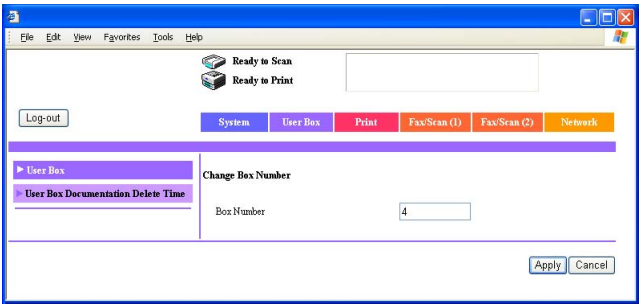
4 Click the [Set].

5 Click the [Change Box Number].



- To change the User Box Name, click [Change User Box Name].
- To change the Document Name, click [Change File Name].
- To change the User Box Password, click [Change User Box Password]. For the procedure to change the User Box Password, see steps 8 through 11.
- To delete the User Box, click [User Box Delete].
- To delete the User Box document, click [Document Delete] or [Delete All documents].

6 Type the new User Box Number.

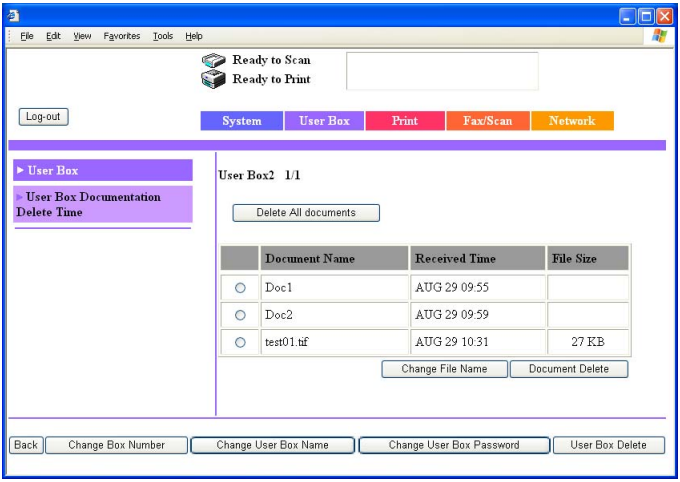


7 Click the [Apply].

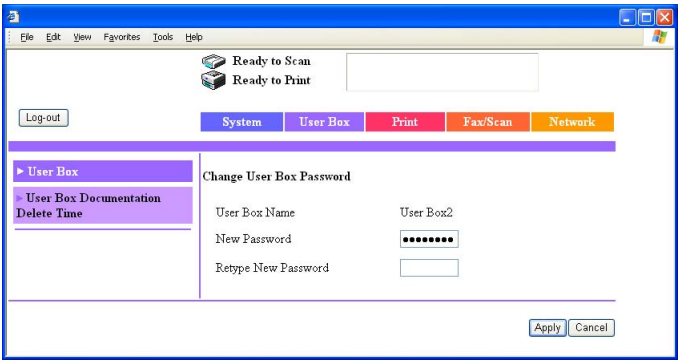
? What if the User Box Number entered is duplicated?

➔ If the User Box Number entered is duplicated, a message will appear that tells that the User Box Number entered cannot be used. Click [OK] and type a new User Box Number that is not duplicated.

8 Click the [Change User Box Password].



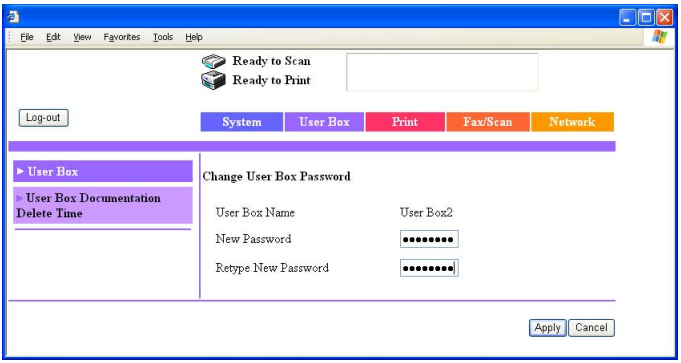
9 Enter a new 8-digit User Box Password in the “New Password” box.



? What precautions should be used when entering the new User Box Password?

➔ Enter a User Box Password that meets the requirements of the Password Rules in the “New Password” box. For details of Password Rules, see “Password Rules” on page 1-11.

10 Enter the new 8-digit User Box Password in the “Retype New Password” box.



11 Click the [Apply].

? What if the User Box Password entered does not meet the requirements of the Password Rules?

➔ If the User Box Password entered does not meet the requirements of the Password Rules, a message appears that tells that the User Box Password entered is wrong. Click [OK] to go back to the screen of step 10. Perform steps 9 and 11 again.

? What if there is a mismatch in the User Box Password between that entered in the New Password box and that entered in the Retype New Password box?

➔ If there is a mismatch in the User Box Password between that entered in the “New Password” box and that entered in the “Retype New Password” box, a message appears that tells that there is a mismatch in the passwords. Click [OK] to go back to the screen of step 10. Enter the correct User Box Password.

Reminder

If a User Box document is deleted or if a User Box document is saved in a User Box that is deleted, the data is deleted by overwriting with 0x00 → 0x00 → 0x00 through the Temporary Data Overwriting function.

2.6 Protecting Data in the HDD

If the optional Hard Disk HD-504 and Security Kit SC-504 are mounted on the machine and when access to the Admin. Management mode by the Administrator of the machine is authenticated, the machine enables the operation for setting and changing the HDD Lock Password and Encryption Key.

Should the HDD be removed unawares, the HDD Lock Password locks the HDD protecting data contained in the HDD. Furthermore, by setting the Encryption Key, the data stored in the HDD is encrypted, thereby protecting the data in the HDD. The HDD Lock Password and Encryption Key entered is displayed as "*."

...

Note

Do not set any number that can easily be guessed from birthdays, employee identification numbers, and the like for the HDD Lock Password and Encryption Key. Try to change the password at regular intervals.

Make sure that nobody but the Administrator of the machine comes to know the HDD Lock Password or Encryption Key.

...

Reminder

When the HDD Lock Password is set, HDD verification is carried out when the machine is started. If the HDD has been improperly replaced with another, or if the HDD Lock Password is yet to be set, a message appears that tells that there is a mismatch between the HDD and the HDD Lock Password. Further, the HDD has the following function. That is, if the HDD is illegally removed, detection of a wrong HDD Lock Password five consecutive times will lock the authentication function. Leak of data can thus be prevented.

When an Encryption Key (encryption word) is set using HDD Encryption Setting, an Encryption Key with a key length of 128 bits is generated using the SHA-1 algorithm. The generated encryption key is used to encrypt or decrypt data through AES encryption algorithm.

2.6.1 Setting the HDD Lock Password

...

Note

When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. Be sure to allow an interval of 10 sec. or more in order to ensure correct operations.
Turn off the sub power switch → Turn off the main power switch → Turn on the main power switch → Turn on the sub power switch

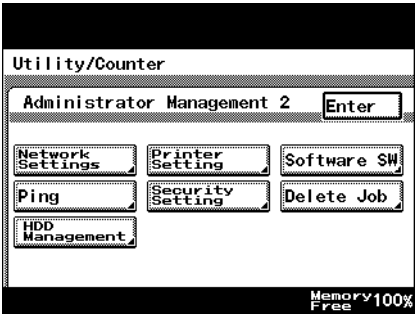
Do not leave the machine with the Admin. Management mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin. Management mode.

<Setting can be made only from the control panel>

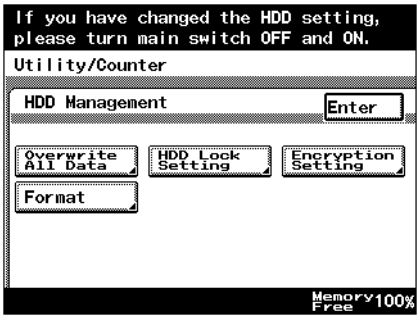
✔ For the procedure to call the Administrator Management 2 to the display, see steps 1 and 2 of "Setting the Enhance Security function" on page 2-10.

1 Call the Administrator Management 2 to the screen from the control panel.

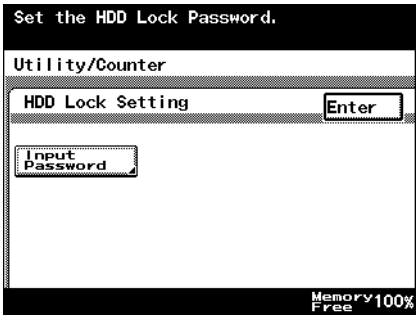
2 Touch [HDD Management].



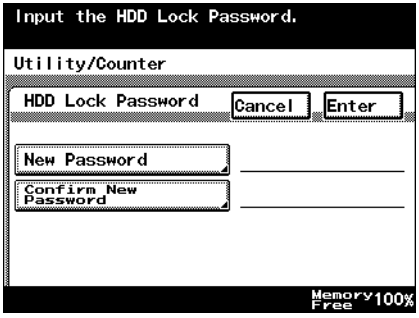
3 Touch [HDD Lock Setting].



4 Touch [Input Password].

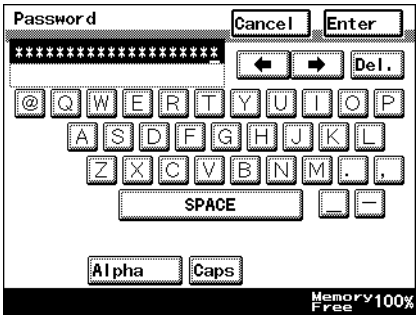


5 Touch [New Password].



6 Enter the 20-digit HDD Lock Password from the keyboard and keypad.

- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Cancel] to go back to the HDD Management screen.



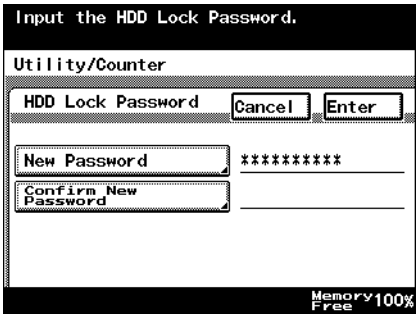
7 Touch [Enter].

? What happens if the HDD Lock Password entered does not meet the requirements of Password Rules?

➔ If the HDD Lock Password entered does not meet the requirements of Password Rules, a message appears that tells that the HDD Lock Password entered is wrong. Enter the correct HDD Lock Password. For details of Password Rules, see “Password Rules” on page 1-11.

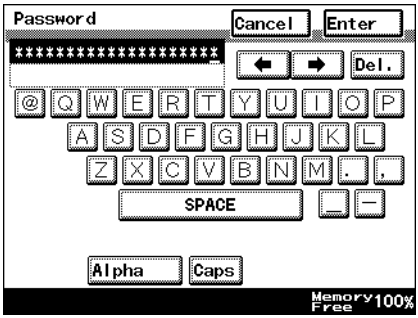
➔ To change the HDD Lock Password, see “Changing the HDD Lock Password” on page 2-30.

8 Touch [Confirm New Password].



9 Enter the 20-digit HDD Lock Password from the keyboard and keypad.

- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Cancel] to go back to the HDD Management screen.

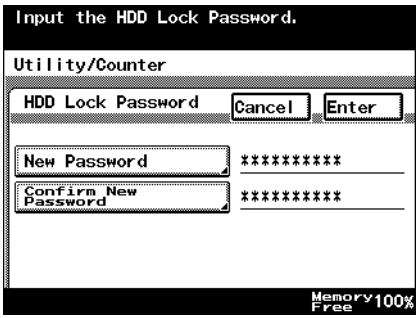


10 Touch [Enter].

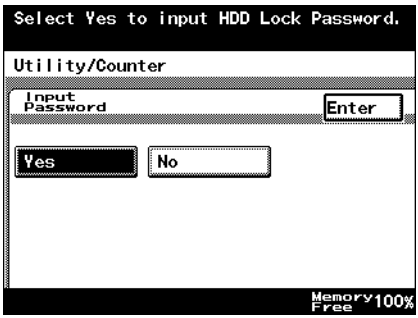
? What if there is a mismatch in the HDD Lock Passwords entered?

→ If there is a mismatch in the HDD Lock Passwords entered, a message appears that tells that the HDD Lock Password entered is wrong. Touch [Enter] and perform steps 5 through 10 again.

11 Touch [Enter].

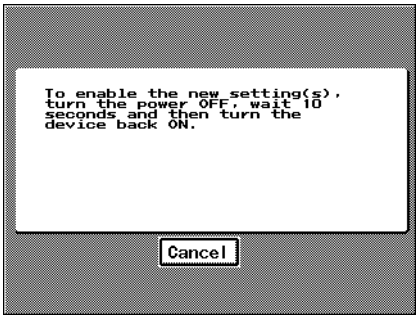


12 A message appears that prompts you to determine whether you want to register the password. Touch [Yes] if you register the password.



13 Touch [Enter].

14 Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch.



...

Note

NEVER forget the HDD Lock Password set through the above procedure. The HDD Lock Password must be entered when changing canceling the HDD Lock Password.

2.6.2 Changing the HDD Lock Password

Note

When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. Be sure to allow an interval of 10 sec. or more in order to ensure correct operations.
Turn off the sub power switch → Turn off the main power switch → Turn on the main power switch → Turn on the sub power switch

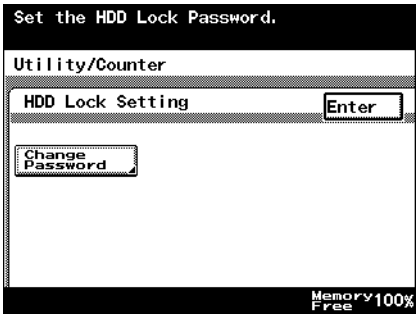
Do not leave the machine with the Admin. Management mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin. Management mode.

<Setting can be made only from the control panel>

✔ To call the HDD Lock Setting screen to the display, see steps 1 through 3 of "Setting the HDD Lock Password" on page 2-25.

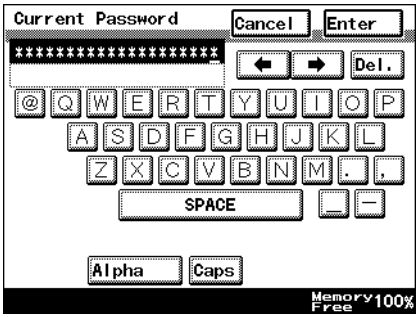
1 Call the HDD Lock Setting screen to the display from the control panel.

2 Touch [Change Password].



3 Enter the currently registered 20-digit HDD Lock Password from the keyboard and keypad.

- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Cancel] to go back to the HDD Setting screen.

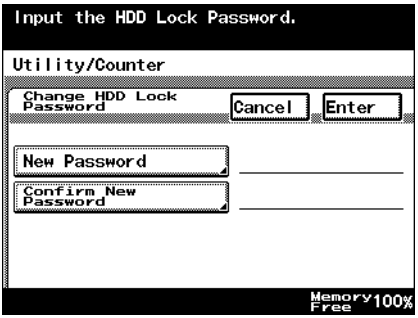


4 Touch [Enter].

? What happens if there is a mismatch in the HDD Lock Passwords?

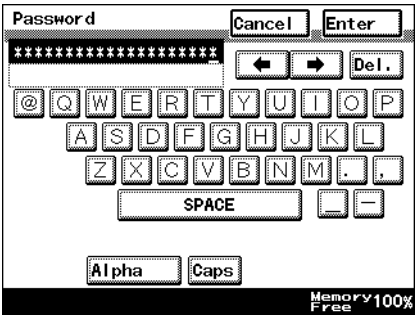
→ If there is a mismatch in the HDD Lock Passwords, a message appears that tells that the HDD Lock Password entered is wrong. Enter the correct HDD Lock Password.

5 Touch [New Password].



6 Enter the 20-digit HDD Lock Password from the keyboard and keypad.

- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Cancel] to go back to the HDD Setting screen.

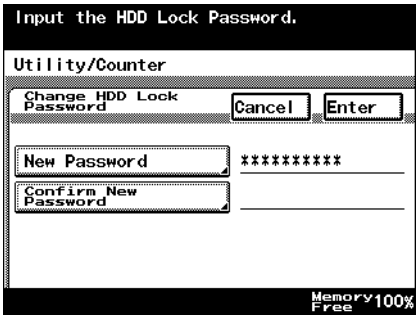


7 Touch [Enter].

? What happens if the HDD Lock Password entered does not meet the requirements of Password Rules?

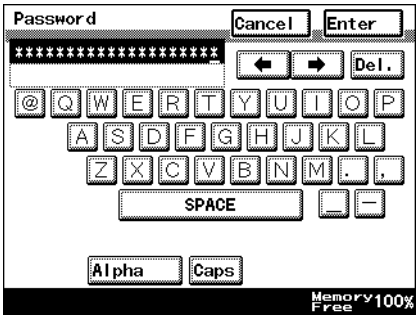
→ If the HDD Lock Password entered does not meet the requirements of Password Rules, a message appears that tells that the HDD Lock Password entered is wrong. Enter the correct HDD Lock Password. For details of Password Rules, see “Password Rules” on page 1-11.

8 Touch [Confirm New Password].



9 Enter the 20-digit HDD Lock Password from the keyboard and keypad.

- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Cancel] to go back to the HDD Management screen.

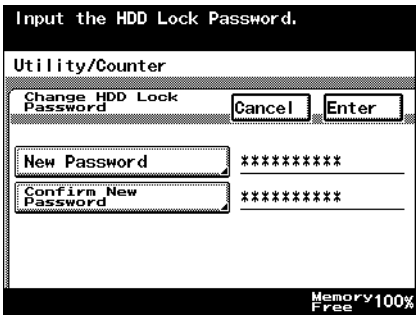


10 Touch [Enter].

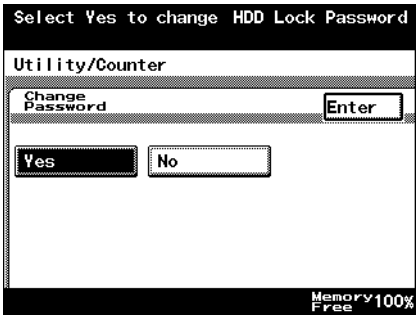
? What if there is a mismatch in the HDD Lock Passwords entered?

→ If there is a mismatch in the HDD Lock Passwords entered, a message appears that tells that the HDD Lock Password entered is wrong. Touch [Enter] and perform steps 5 through 10 again.

11 Touch [Enter].

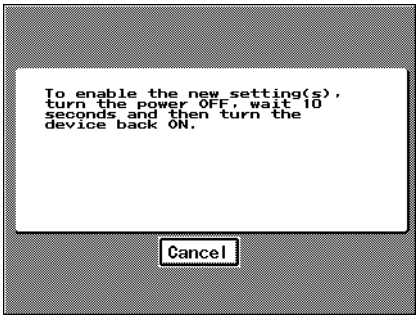


12 A message appears that prompts you to determine whether you want to change the password. Touch [Yes] if you want to change the password.



13 Touch [Enter].

14 Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch.



...

Note

NEVER forget the HDD Lock Password set through the above procedure. The HDD Lock Password must be entered when changing canceling the HDD Lock Password.

2.6.3 Setting the Encryption Key (encryption word)

...

Note

When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. Be sure to allow an interval of 10 sec. or more in order to ensure correct operations.
Turn off the sub power switch → Turn off the main power switch → Turn on the main power switch → Turn on the sub power switch

NEVER forget the Encryption Key set through the above procedure. The Encryption Key must be entered when changing canceling the Encryption Key .

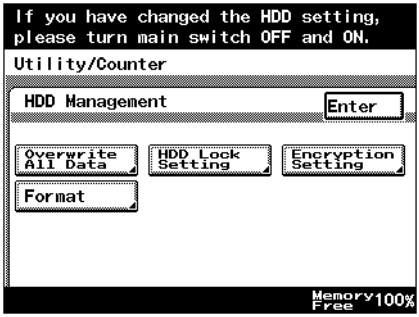
Do not leave the machine with the Admin. Management mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin. Management mode.

<Setting can be made only from the control panel>

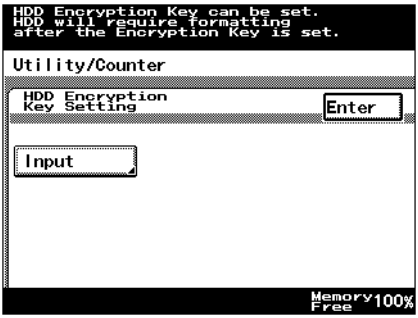
✔ For the procedure to call the HDD Management to the display, see steps 1 and 2 of "Setting the HDD Lock Password" on page 2-25.

1 Call the HDD Management screen to the display from the control panel.

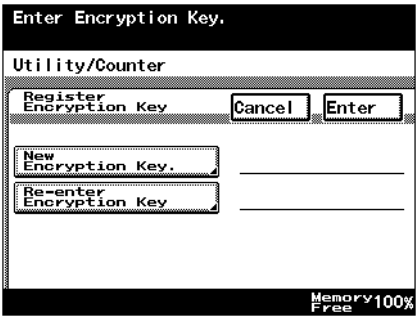
2 Touch [Encryption Setting].



3 Touch [Input].

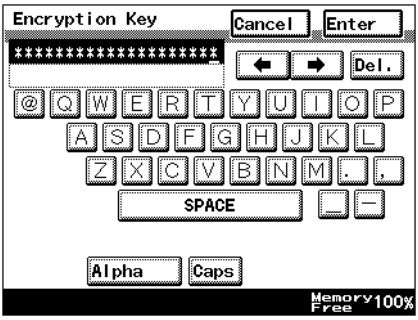


4 Touch [New Encryption Key].



5 Enter the new 20-digit Encryption Key from the keyboard and keypad.

- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Cancel] to go back to the HDD Management screen.

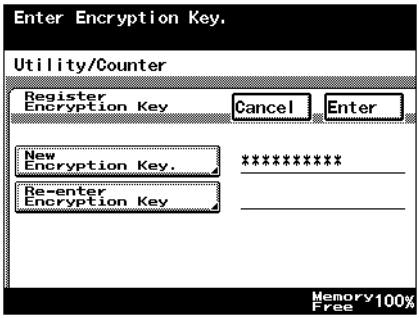


6 Touch [Enter].

? What happens if the Encryption Key entered does not meet the requirements of Password Rules?

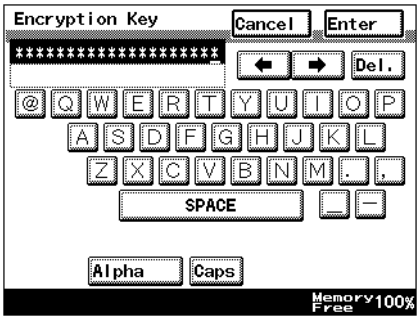
➔ If the Encryption Key entered does not meet the requirements of Password Rules, a message appears that tells that the Encryption Key entered is wrong. Enter the correct Encryption Key. For details of Password Rules, see “Password Rules” on page 1-11.

7 Touch [Re-enter Encryption Key].



8 Enter the 20-digit Encryption Key from the keyboard and keypad.

- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Cancel] to go back to the HDD Management screen.

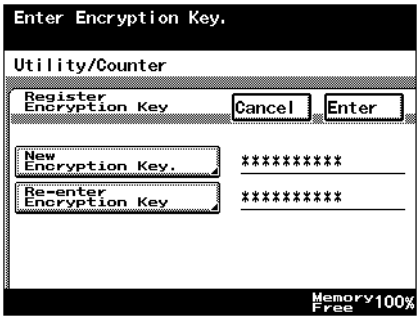


9 Touch [Enter].

? What if there is a mismatch in the Encryption Keys entered?

➔ If there is a mismatch in the Encryption Keys entered, a message appears that tells that the Encryption Key entered is wrong. Touch [Enter] and perform steps 4 through 9 again.

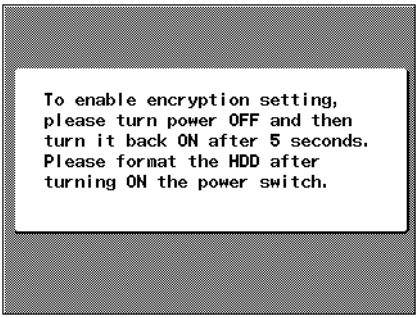
10 Touch [Enter].



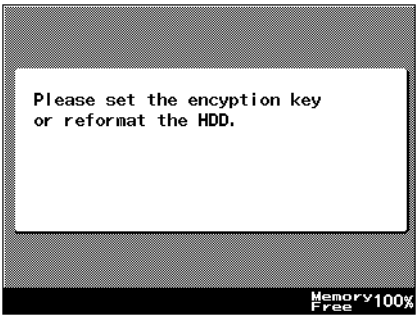
11 A message will appear, asking whether you want to register the Encryption Key or not. Touch [Yes], if you are sure to register the Encryption Key.

12 Touch [Enter].

13 Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch.


To enable encryption setting,
please turn power OFF and then
turn it back ON after 5 seconds.
Please format the HDD after
turning ON the power switch.

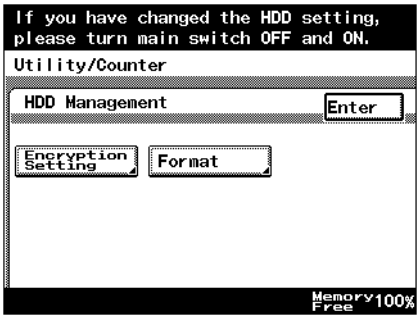
14 The following screen appears after the machine has been restarted.



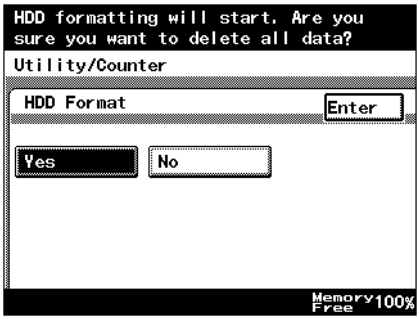
15 Call the Admin. Management screen to the display from the control panel.

– For the procedure to call the Admin. Management mode to the display, see steps 1 through 4 of “Accessing the Admin. Management mode” on page 2-2.

16 Touch [Format].

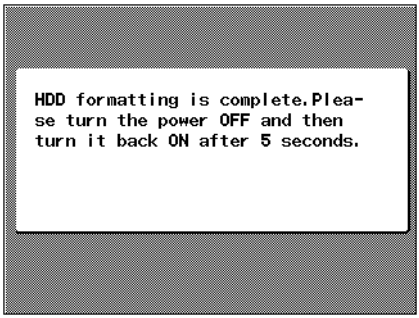


17 Touch [Yes].



18 Touch [Enter].

19 When HDD formatting is completed, a message will appear prompting you to turn OFF and ON the main power switch. Now, turn OFF the main power switch, and then turn it ON again.



2.6.4 Changing the Encryption key

...

Note

When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. Be sure to allow an interval of 10 sec. or more in order to ensure correct operations.
Turn off the sub power switch → Turn off the main power switch → Turn on the main power switch → Turn on the sub power switch

NEVER forget the Encryption Key set through the above procedure. The Encryption Key must be entered when changing canceling the Encryption Key .

Do not leave the machine with the Admin. Management mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin. Management mode.

<Setting can be made only from the control panel>

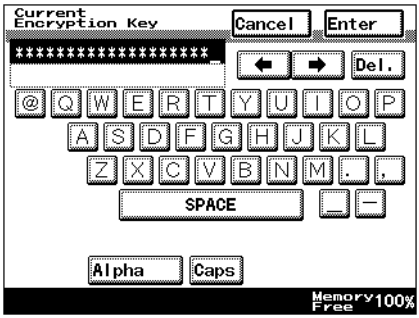
✔ For the procedure to call the Encryption Setting to the display, see steps 1 and 2 of "Setting the Encryption Key (encryption word)" on page 2-34.

1 Call the Encryption Setting screen to the display from the control panel.

2 Touch [Change].

3 Enter the currently registered 20-digit Encryption Key from the keyboard and keypad.

- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Cancel] to go back to the HDD Management screen.

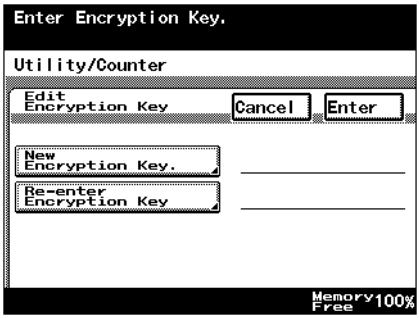


4 Touch [Enter].

? What if there is a mismatch in the Encryption Keys entered?

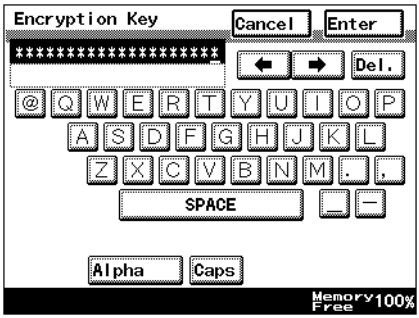
→ If there is a mismatch in the Encryption Keys entered, a message appears that tells that the Encryption Key entered is wrong. Touch [Enter] and enter the correct Encryption Key.

5 Touch [New Encryption Key].



6 Enter the new 20-digit Encryption Key from the keyboard and keypad.

- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Cancel] to go back to the HDD Management screen.

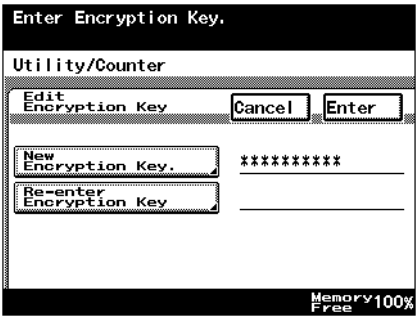


7 Touch [Enter].

? What happens if the Encryption Key entered does not meet the requirements of Password Rules?

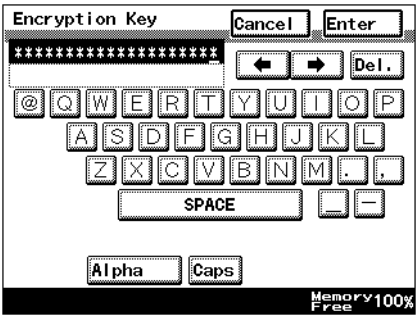
→ If the Encryption Key entered does not meet the requirements of Password Rules, a message appears that tells that the Encryption Key entered is wrong. Enter the correct Encryption Key. For details of Password Rules, see “Password Rules” on page 1-11.

8 Touch [Re-enter Encryption Key].



9 Enter the 20-digit Encryption Key from the keyboard and keypad.

- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Cancel] to go back to the HDD Management screen.

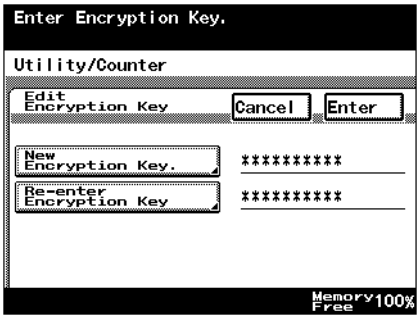


10 Touch [Enter].

? What if there is a mismatch in the Encryption Keys entered?

→ If there is a mismatch in the Encryption Keys entered, a message appears that tells that the Encryption Key entered is wrong. Touch [Enter] and perform steps 5 through 10 again.

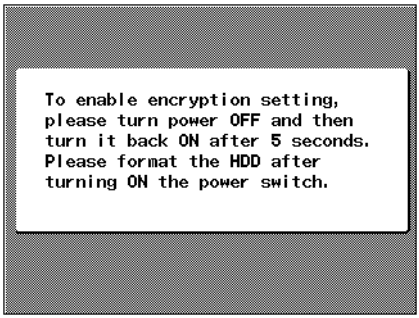
11 Touch [Enter].



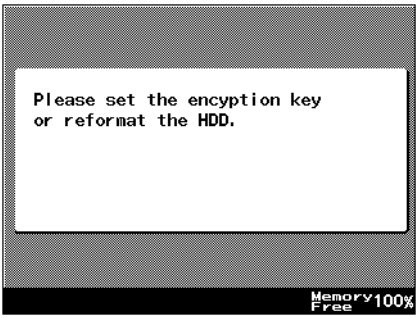
12 A message will appear, asking whether you want to change the Encryption Key or not. Touch [Yes], if you are sure to change the Encryption Key.

13 Touch [Enter].

14 Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch.


To enable encryption setting,
please turn power OFF and then
turn it back ON after 5 seconds.
Please format the HDD after
turning ON the power switch.

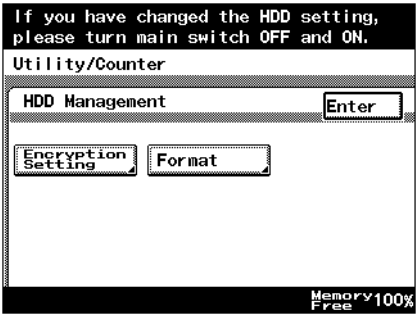
15 The following screen appears after the machine has been restarted.



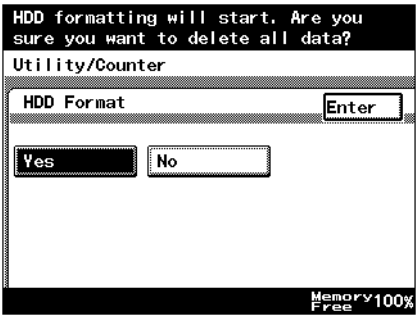
16 Call the Admin. Management screen to the display from the control panel.

– For the procedure to call the Admin. Management mode to the display, see steps 1 through 4 of “Accessing the Admin. Management mode” on page 2-2.

17 Touch [Format].

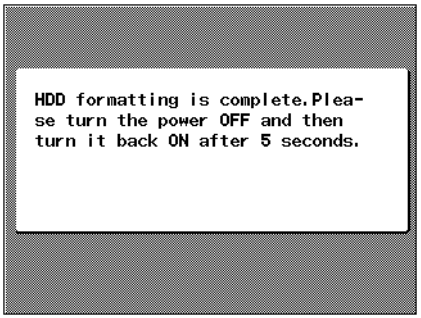


18 Touch [Yes].



19 Touch [Enter].

20 When HDD formatting is completed, a message will appear prompting you to turn OFF and ON the main power switch. Now, turn OFF the main power switch, and then turn it ON again.



2.7 Overwrite All Data Function

When access to the Admin. Management mode by the Administrator of the machine via the control panel is authenticated, the machine enables setting of the operation of the Overwrite All Data function.

When the machine is to be discarded, or use of a leased machine is terminated at the end of the leasing contract, the Overwrite All Data function overwrites and erases all data stored in all spaces of the HDD. The function also resets all passwords saved in the NVRAM to factory settings, preventing leak of data.

The Overwrite All Data function clears the following types of data.

Types of Data Cleared	Description
Enhance Security function	Clears the current settings, resetting them to the default ones.
User Box Password/file	Deletes the User Box Password and all files saved in the user box.
Swap data	Deletes all swap data generated in a copy, PC print, or Secure Print Document that is too large in size to fit in the RAM space, representing part of the image files stored in the HDD.
Image files	Deletes overlay image files and all image files stored in the HDD.
Destination recipient data files	Deletes all destination recipient data including e-mail addresses and telephone numbers
HDD Lock Password	Clears the currently set password.
Encryption Key	Clears the currently set Encryption Key.
Administrator Code (Administrator Password)	Clears the currently set password, resetting it to the factory setting

Detail

The Overwrite All Data function overwrites and deletes data stored in all spaces of the HDD through the following method:
0x00 → 0xFF → 0x00 → 0xFF → 0x00 → 0xFF → 0xAA → verify

2.7.1 Executing Overwrite All Data

...

Note

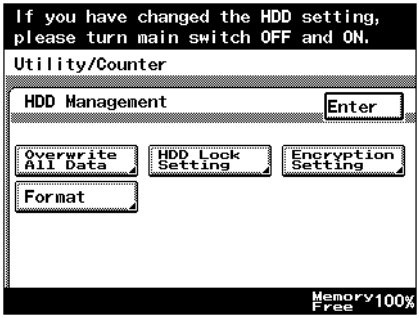
Do not leave the machine with the Admin. Management mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin. Management mode.

<Setting can be made only from the control panel>

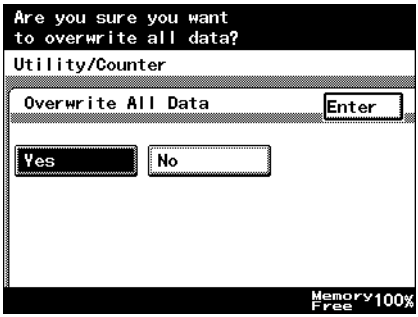
✔ For the procedure to call the HDD Management to the display, see steps 1 and 2 of "Setting the HDD Lock Password" on page 2-25.

1 Call the HDD Management to the screen from the control panel.

2 Touch [Overwrite All Data].



3 Touch [Yes].



4 Touch [Enter].

2.8 Network Setting Function

When access to the Admin. Management mode by the Administrator of the machine is authenticated, the machine allows the settings to be made of the IP address and for use of the machine as a network printer.

2.8.1 Setting the IP Address

...

Note

Do not leave the machine with the Admin. Management mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin. Management mode.

<From the Control Panel>

✔ For the procedure to call the Admin. 2 to the display, see steps 1 and 2 of “Setting the Enhance Security function” on page 2-10.

1 Call the Admin. 2 to the screen from the control panel.

2 Touch [Network Settings].

3 Touch [Basic Settings].

4 Touch [DHCP].

5 Touch [IP Input].

– If [Auto-Obtain] is selected, the IP address is automatically acquired.

6 Touch [IP Address Setting].

7 Set the IP Address.

8 Touch [Enter].

<From PageScope Web Connection>

✔ For the procedure to access the Admin. Management mode, see “Accessing the Admin. Management mode” on page 2-2.

1 Start PageScope Web Connection and access the Admin. Management mode.

2 Click the [Network] tab and the [TCP/IP] menu.

3 Set the IP address.

4 Click the [Apply].

2.8.2 Making the NetWare setting

Note

Do not leave the machine with the Admin. Management mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin. Management mode.

<From PageScope Web Connection>

✔ For the procedure to access the Admin. Management mode, see “Accessing the Admin. Management mode” on page 2-2.

1 Start PageScope Web Connection and access the Admin. Management mode.

2 Click the [Network] tab and the [NetWare] menu.

3 Make the necessary settings.

4 Click the [Apply].

2.8.3 Making the Windows print (NetBIOS) setting

Note

Do not leave the machine with the Admin. Management mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin. Management mode.

<From PageScope Web Connection>

✔ For the procedure to access the Admin. Management mode, see “Accessing the Admin. Management mode” on page 2-2.

1 Start PageScope Web Connection and access the Admin. Management mode.

2 Click the [Network] tab and the [Windows] menu.

3 Make the necessary settings.

4 Click the [Apply].

2.8.4 Making the AppleTalk setting

Note

Do not leave the machine with the Admin. Management mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin. Management mode.

<From PageScope Web Connection>

✔ For the procedure to access the Admin. Management mode, see “Accessing the Admin. Management mode” on page 2-2.

1 Start PageScope Web Connection and access the Admin. Management mode.

2 Click the [Network] tab and the [AppleTalk] menu.

3 Make the necessary settings.

4 Click the [Apply].

3 User Operations

3 User Operations

3.1 Secure Print Function

The Secure Print function allows a Secure Print specified by a corresponding password from the PC to be used in the condition registered in the machine.

To access a Secure Print document, authentication is performed through an 8-digit password that verifies an authenticated user of the Secure Print document. The password entered for the authentication purpose appears as "*" or "●" on the display. When the Enhance Security function is set to [ON], the number of times in which authentication fails is counted.

Note

Enter the Secure Print ID and Secure Print Password through the printer driver on the PC side. The Secure Print Password entered is displayed as "."*

The Secure Print Password must be the one consisting of 8 digits and meeting the Password Rules requirements. Any Secure Print, the password for which does not meet the Password Rules requirements, will not be registered in the machine. For details of Password Rules, see "Password Rules" on page 1-11.

3.1.1 Accessing the Secure Print

Note

For the Secure Print ID, enter the one that has been set on the printer driver side.

If a wrong Secure Print ID is entered, a message appears that tells that there is a mismatch in the Secure Print ID and the machine does not display the target Secure Print Document. Enter the correct Secure Print ID.

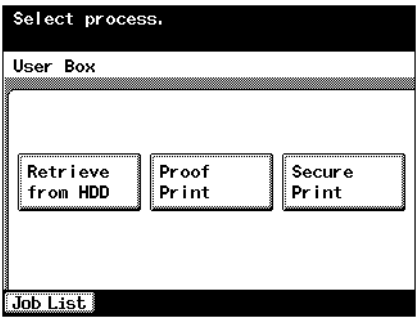
The machine rejects any Secure Print Password that consists of less than 8 digits.

For the Secure Print Password, enter the 8-digit one set on the printer driver side.

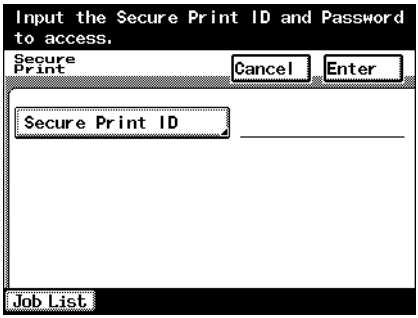
<Setting can be made only from the control panel>

1 Press the [Box] key.

2 Touch [Secure Print].

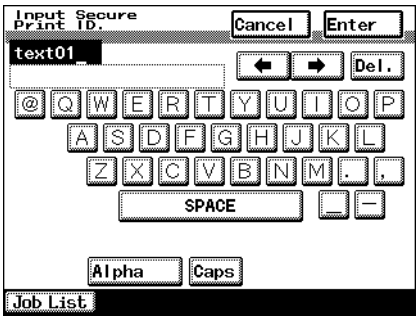


3 Touch [Secure Print ID].



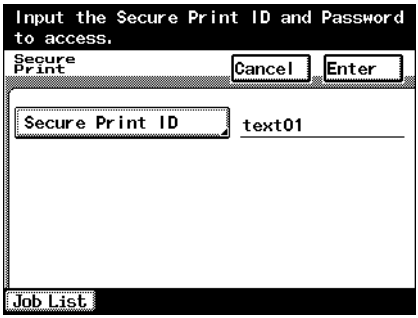
4 Enter the Secure Print ID that consists of up to 8 digits from the keyboard and keypad.

- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Cancel] to go back to the previous screen.

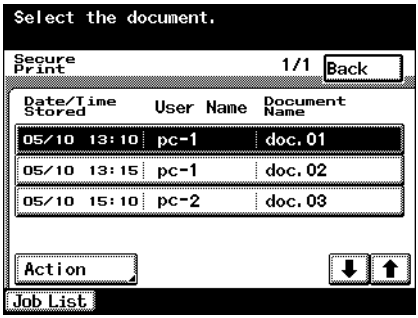


5 Touch [Enter].

6 Touch [Enter].

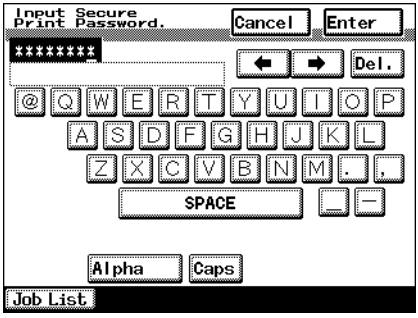


7 Select the target Secure Print and touch [Action].



8 Enter the 8-digit Secure Print Password from the keyboard and keypad.

- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Cancel] to go back to the previous screen.



9 Touch [Enter].

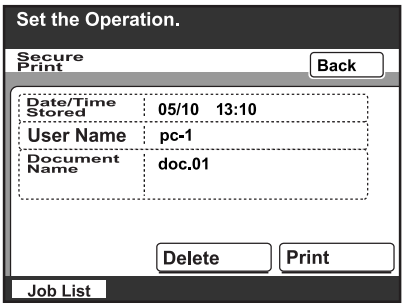
? What if there is a mismatch of the Secure Print Password relative to the Secure Print ID?

➔ If there is a mismatch of the Secure Print Password relative to the Secure Print ID, a message appears that tells that the authentication has been unsuccessful. Touch [OK] and enter the correct Secure Print Password.

➔ If the Enhance Security function is set to [ON], the machine counts entry of a wrong Secure Print Password as unauthorized access. If a wrong Secure Print Password is entered three times, a message appears that tells that authentication has been unsuccessful for any subsequent authentication attempt. The machine is then set into an access lock state, rejecting any access to Secure Print. To cancel the access lock state, the Administrator of the machine must perform the Unlock operation. Contact the Administrator of the machine.

10 Check the document information and touch [Print].

– If [Delete] is touched, a message appears that prompts you to confirm if the Secure Print selected may be deleted. Touch [Yes] if the Secure Print may be deleted.



? What happens if Secure Print is deleted?

➔ If Secure Print is deleted, the data is overwritten and deleted with 0x00 → 0x00 → 0x00 through the Temporary Data Overwriting function.

11 Touch [Enter].

Detail

When printing is executed for Secure Print, the Secure Print is automatically deleted. When Secure Print is deleted, the data is overwritten and deleted with 0x00→ 0x00→ 0x00 through the Temporary Data Overwriting function.

3.2 User Box Function

The machine allows all users to register User Boxes and operate to make changes for the boxes. It also allows the user to acquire an image file stored in the User Box and print it as necessary.

User Box prepares a User Box in the HDD as a space for saving image files. Up to 115 User Boxes can be registered.

Access to a User Box is authenticated using an 8-digit User Box Password. The User Box Password entered is displayed as "*" or "●." When the Enhance Security function is set to [ON], the number of times in which authentication fails is counted.

3.2.1 Setting the User Box

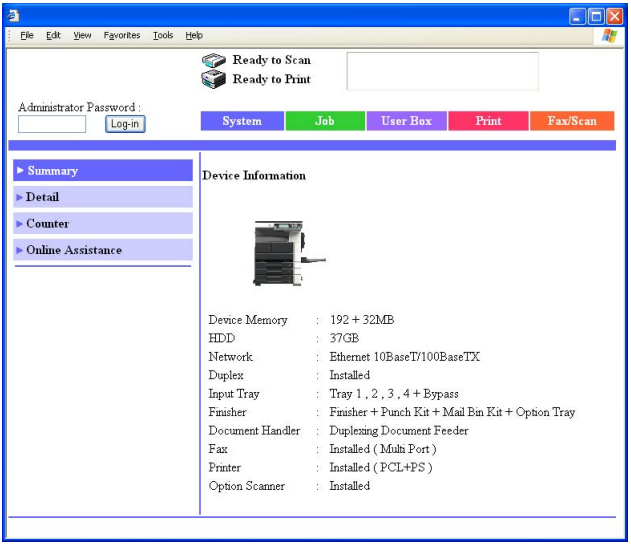
<Setting can be made only from PageScope Web Connection>

1 Start the Web browser.

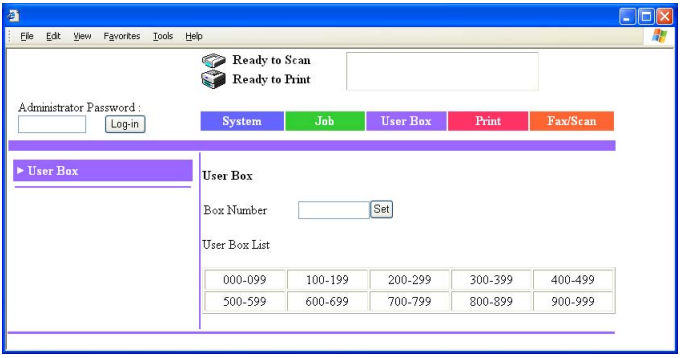
2 Enter the IP address of the machine in the address bar.

3 Press the [Enter] key to start PageScope Web Connection.

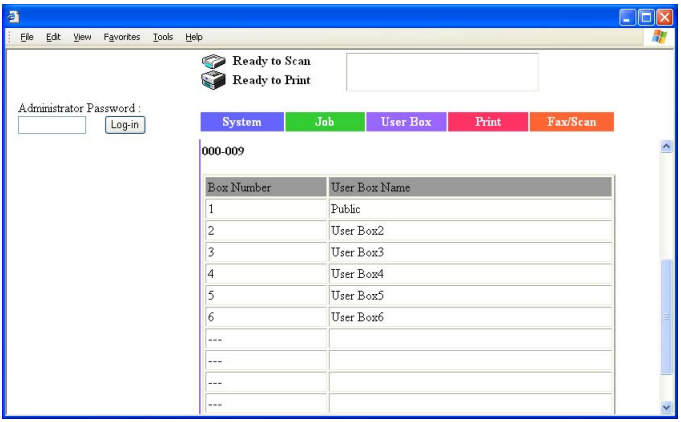
4 Click the [User Box] tab.



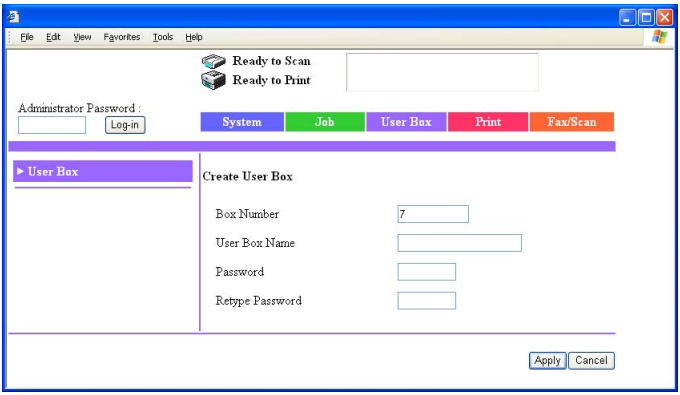
5 Click the target index of the User Box List.



6 Click "---" of "Box Number."



7 Type the User Box Number in the “Box Number” field.



– Even if the User Box Number entered falls outside the range of the number index selected from User Box List, the machine does not sort the User Box into the correct number range index.

? What precautions should be used when registering a User Box Number?

➔ A User Box Number that already exists cannot be registered.

8 Enter a User Box Name that may consist of up to 20 characters in the “User Box Name” box.

? What precautions should be used when registering a User Box Name?

➔ When setting a User Box Name, do not use “Public” for the User Box Name to avoid confusion with the “Public User Box” previously registered.

9 Enter an 8-digit User Box Password in the “Password” box.

? What precautions should be used when entering a User Box Password?

➔ Enter a User Box Password that meets the requirements of the Password Rules in the “Password” box. For details of Password Rules, see “Password Rules” on page 1-11.

10 Enter the 8-digit User Box Password in the “Retype Password” box.

11 Click the [Apply].

...

Note

If the User Box Number entered is duplicated, a message will appear that tells that the User Box Number entered cannot be used. Click [OK] and type a new User Box Number that is not duplicated.

If an illegal User Box Name is entered, a message appears that tells that an illegal User Box Name has been entered. Click [OK] and enter the correct User Box Name.

If the User Box Password entered in the "Password" box does not meet the requirements of the Password Rules, a message appears that tells that the User Box Password entered is wrong. Click [OK] and enter the correct User Box Password.

If there is a mismatch in the User Box Password between that entered in the "Password" box and that entered in the "Retype Password" box, a message appears that tells that the User Box Password entered in the "Retype Password" box is wrong. Click [OK] and enter the correct User Box Password.

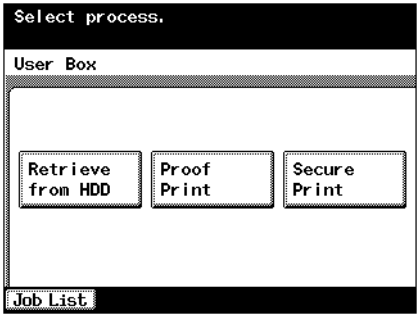
If a User Box has been created, inform the Administrator of the machine of the User Box Number and User Box Name as soon as possible.

3.2.2 Accessing a User Box document

<From the Control Panel>

1 Press the [Box] key.

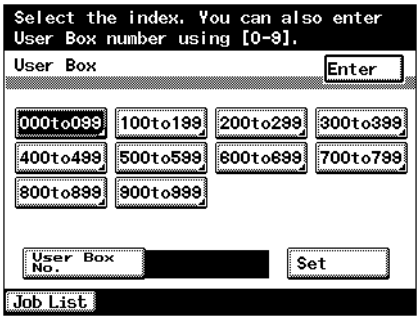
2 Touch [Retrieve from HDD].



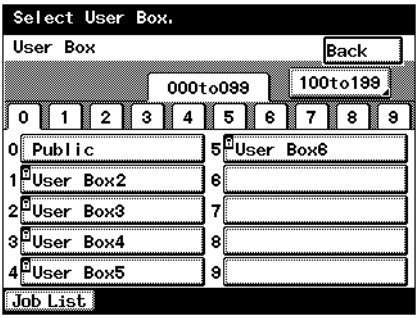
3 Select the desired User Box.

- If the User Box is to be selected from the index, perform steps 4 and 5.
- If the User Box Number is to be directly entered, perform steps 6 and 7.

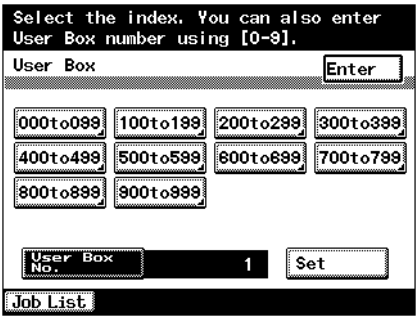
4 Touch the relevant index.



5 Select the target User Box.



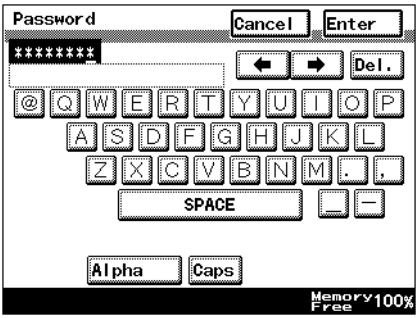
6 Touch [User Box No.] and type the target User Box Number from the 10-Key Pad.



7 Touch [Set].

8 Enter the 8-digit User Box Password from the keyboard and keypad.

- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Cancel] to go back to the User Box selection screen.



9 Touch [Enter].

? What if there is a mismatch in the User Box Passwords?

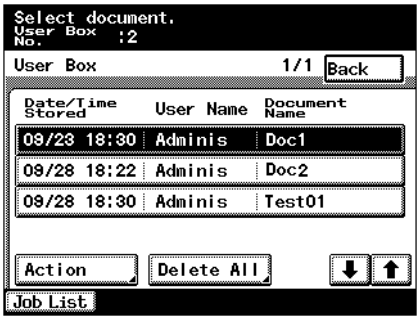
→ If there is a mismatch in the User Box Passwords, a message appears that tells that the User Box Password entered is wrong. Enter the correct User Box Password.

➔ If the Enhance Security function is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong User Box Password is entered three times, a message appears that tells that the machine rejects any access to the User Box for any subsequent authentication attempt. The machine is then set into an access lock state. To cancel the access lock state, the Administrator of the machine must perform the Unlock operation. Contact the Administrator of the machine.

10 Select the target User Box document.

– To delete all User Box documents contained in the User Box selected, touch [Delete All].

? What happens when Delete All is executed?



➔ If [Delete All] is executed, the data is deleted by overwriting with 0x00 → 0x00 → 0x00 through the Temporary Data Overwriting function.

11 Touch [Action].

12 Select the desired function.

– To print the User Box document, touch [Print].
– To change the User Box document name, touch [Change Name].
– To deliver the User Box document over a network, touch [Route].
– To delete the User Box document, touch [Delete].

...

Reminder

If the destination is to be specified using the corresponding one-touch key for executing [Route] from the control panel, always check that the destination is correct to make sure that the data is sent to the correct destination.

If the destination is to be specified through direct input for executing [Route] from the control panel, always check that the destination is correct to make sure that the data is sent to the correct destination.

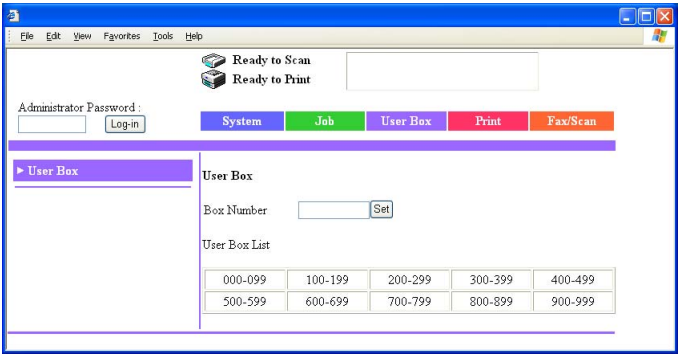
If the User Box document is deleted, it is deleted by overwriting with 0x00 → 0x00 → 0x00 through the Temporary Data Overwriting function.

<From PageScope Web Connection>

✔ For the procedure to show the [User Box] tab on the screen, see steps 1 through 4 of “Setting the User Box” on page 3-6.

1 Using PageScope Web Connection, display the [User Box] tab.

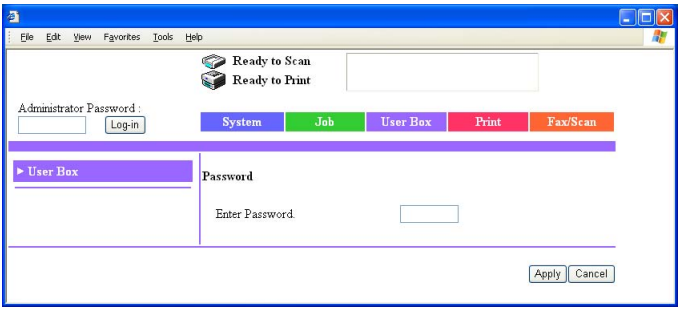
2 Type the desired User Box Number in the “Box Number” field.



– Clicking a number range index under User Box List will display a list of boxes having the box numbers that fall within the number range index.

3 Click the [Set].

4 Enter the 8-digit User Box Password.



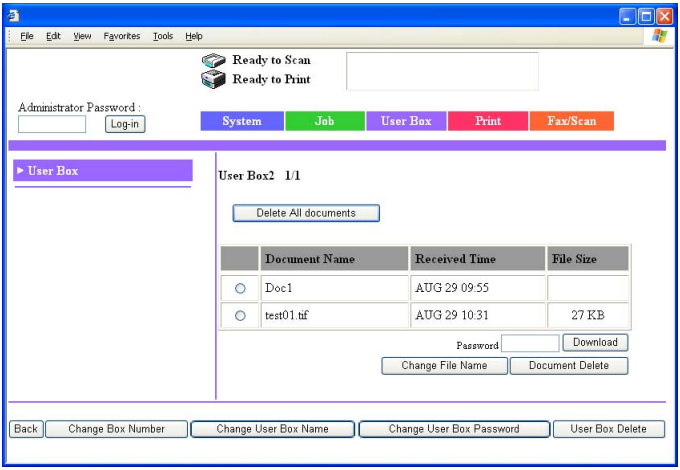
5 Click the [Apply].

? What if there is a mismatch in the User Box Passwords?

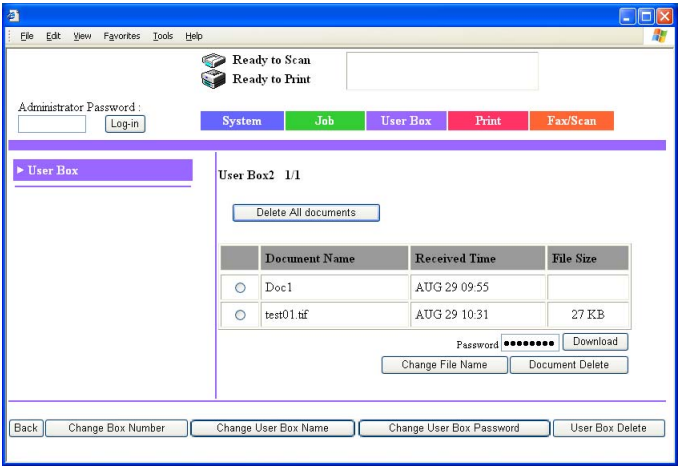
➔ If there is a mismatch in the User Box Passwords, a message appears that tells that there is a mismatch in the User Box Passwords. Click [OK] and enter the correct the User Box Password.

➔ If the Enhance Security function is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong User Box Password is entered three times, a message appears that tells that the machine rejects any access to the User Box for any subsequent authentication attempt. The machine is then set into an access lock state. To cancel the access lock state, the Administrator of the machine must perform the Unlock operation. Contact the Administrator of the machine.

6 Click the radio button of the target document.



7 Enter the 8-digit User Box Password in the “Password” box and click [Download].



– To change the User Box Number, click [Change Box Number]. For details of how to change the User Box Name, see “Changing the User Box Number and User Box Password” on page 3-18.
– To change the User Box Name, click [Change User Box Name].
– To change the User Box Password, click [Change User Box Password]. For details of how to change the User Box Password, see “Changing the User Box Number and User Box Password” on page 3-18.
– To change the Document Name, click [Change File Name].
– To delete the User Box document, click [Document Delete] or [Delete All document].
– To delete the User Box, click [User Box Delete].

? Which password should be entered in the Password box?

➔ Enter the User Box Password in the “Password” box.

➔ If a wrong User Box Password is entered in the “Password” box, a message appears that tells that the User Box Password entered is wrong. Click [OK] and perform steps 6 and 7 again.

➔ If the Enhance Security function is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong User Box Password is entered three times, a message appears that tells that the machine rejects any access to the User Box for any subsequent authentication attempt. The machine is then set into an access lock state. To cancel the access lock state, the Administrator of the machine must perform the Unlock operation. Contact the Administrator of the machine.

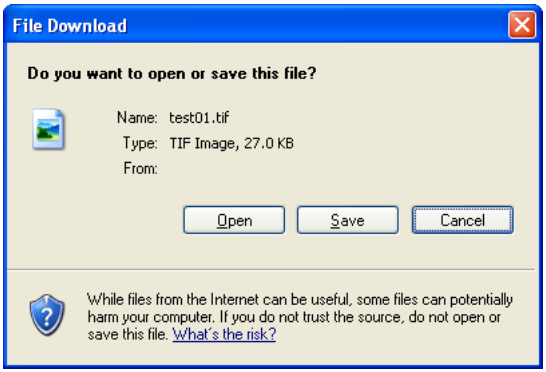
? What precautions should be used when changing a User Box Name?

➔ When a User Box Name is to be changed, do not use “Public” for the User Box Name to avoid confusion with the “Public User Box” previously registered.

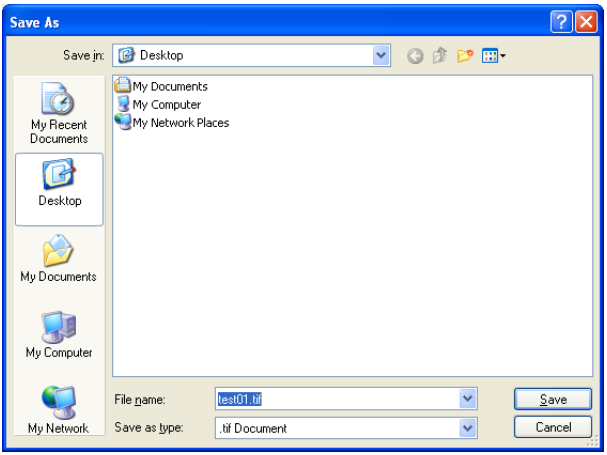
? What happens if a User Box document is deleted or a User Box document is stored in a User Box which is deleted?

➔ If a User Box document is deleted or a User Box document is stored in a User Box which is deleted, the data is deleted by overwriting with 0x00 → 0x00 → 0x00 through the Temporary Data Overwriting function.

8 To save the document, click [Save].


File Download
Do you want to open or save this file?
Name: test01.tif
Type: TIF Image, 27.0 KB
From:
Open
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

9 Specify the destination in which the document is to be saved and the file name. Then, click [Save].



3.2.3 Changing the User Box Number and User Box Password

Note

It is not allowed to duplicate any User Box Number that has previously been registered.

NEVER forget the new User Box Number.

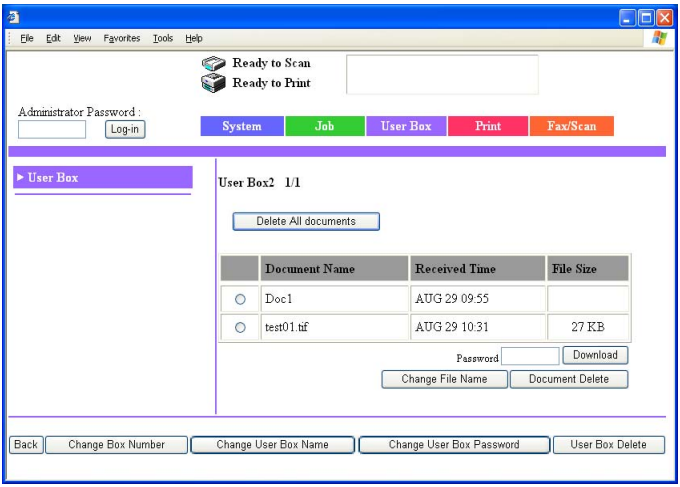
If a User Box Number have been changed, inform the Administrator of the machine of the new User Box Number as soon as possible.

<Setting can be made only from PageScope Web Connection>

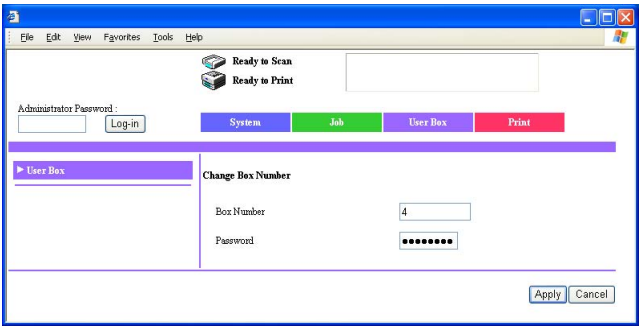
✔ For the procedure to access the User Box, see steps 1 through 5 of "Accessing a User Box document" on page 3-10.

1 Access the User Box through PageScope Web Connection.

2 Click the [Change Box Number].



3 Type the new User Box Number and the currently set 8-digit User Box Password.



4 Click the [Apply].

? What if the User Box Number entered is duplicated?

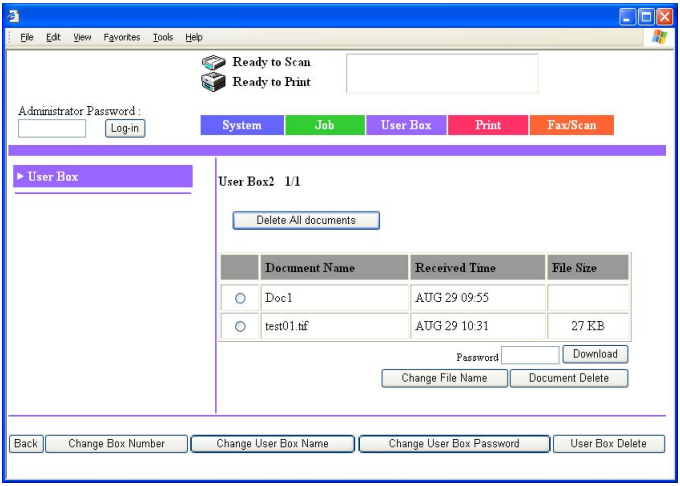
➔ If the User Box Number entered is duplicated, a message will appear that tells that the User Box Number entered cannot be used. Click [OK] and type a new User Box Number that is not duplicated.

? What if there is a mismatch in the User Box Passwords?

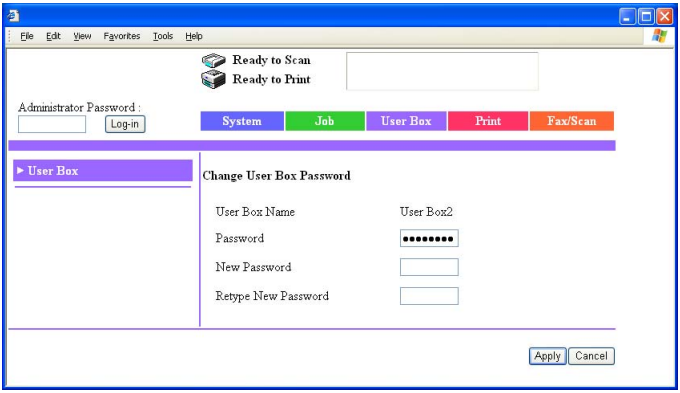
➔ If there is a mismatch in the User Box Passwords, a message appears that tells that there is a mismatch in the User Box Passwords. Click [OK] and enter the correct the User Box Password.

➔ If the Enhance Security function is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong User Box Password is entered three times, a message appears that tells that the machine rejects any access to the User Box for any subsequent authentication attempt. The machine is then set into an access lock state. To cancel the access lock state, the Administrator of the machine must perform the Unlock operation. Contact the Administrator of the machine.

5 Click the [Change User Box Password].



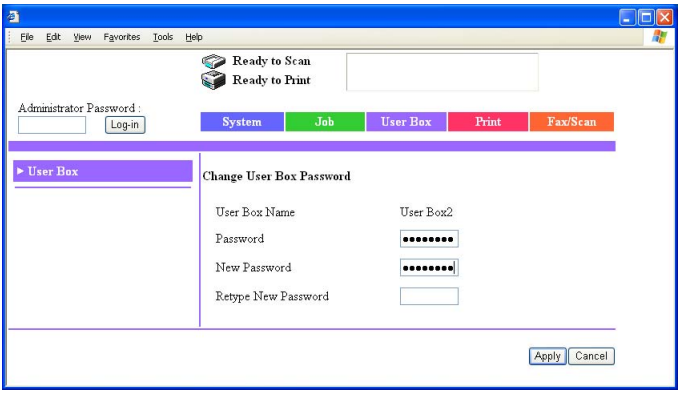
6 Enter the currently set 8-digit User Box Password in the “Password” box.



? Which password should be entered in the Password box?

➔ Enter the currently set User Box Password in the “Password” box.

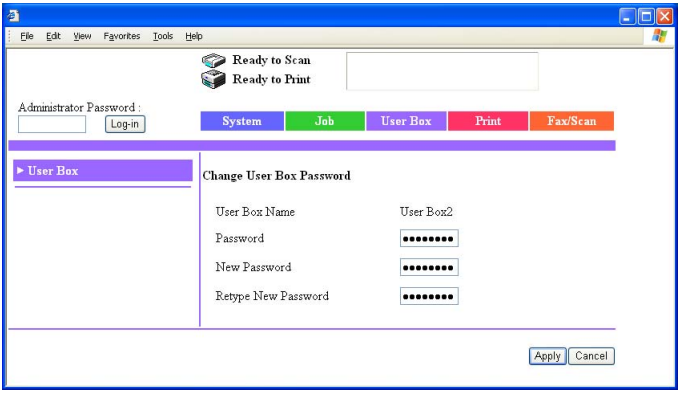
7 Enter a new 8-digit User Box Password in the “New Password” box.



? What precautions should be used when entering the User Box Password in the New Password box?

➔ Enter the User Box Password that meets the requirements of the Password Rules in the “New Password” box. For details of Password Rules, see “Password Rules” on page 1-11.

8 Enter the 8-digit User Box Password in the “Retype New Password” box.



9 Click the [Apply].

...

Note

If there is a mismatch in the User Box Password between that entered in the "Password" box and that registered in the machine, a message appears that tells that the User Box Password entered is wrong. Click [OK] to go back to the screen of step 8. Then, perform the steps 6 through 9 again.

If the Enhance Security function is set to [ON], the machine counts entry of a wrong User Box Password as unauthorized access. If a wrong currently set User Box Password is entered three times, a message appears that tells that the User Box cannot be accessed for any subsequent entry of password. The machine is then set into an access lock state. To cancel the access lock state, the Administrator of the machine must perform the Unlock operation. Contact the Administrator of the machine.

If the User Box Password entered in the "New Password" box does not meet the requirements of the Password Rules, a message appears that tells that the User Box Password entered is wrong. Click [OK] to go back to the screen of step 8. Then, perform the steps 7 through 9 again.

If there is a mismatch in the User Box Passwords between that entered in the "New Password" box and that entered in the "Retype New Password" box, a message appears that tells that there is a mismatch in the User Box Passwords. Click [OK] to go back to the screen of step 8. Perform steps 7 and 9 once again.

KONICA MINOLTA

http://konicaminolta.com

Copyright

A11U-9630-00A

2008 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.